An Roinn Airgeadais
Department of Finance

National Risk Assessment Ireland

Money Laundering, Terrorist Financing, and Proliferation Financing 2026

Prepared by the Department of Finance

Contents

Acronyms

Acronym	Full Form
AI	Artificial Intelligence
AIF	Alternative Investment Fund
AML	Anti-Money Laundering
AMLA	Anti-Money Laundering Authority
AMLAR	Anti-Money Laundering Authority Regulation
AMLCU	Anti-Money Laundering Compliance Unit
AMLD6	Sixth Anti-Money Laundering Directive
AMLR	Anti-Money Laundering Regulation
AMLSC	Anti-Money Laundering Steering Committee
AMON	Anti-Money Laundering Operational Network
APSS	Approved Profit-sharing Schemes
ASP	Accounting Services Provider
ATM	Automated Teller Machine
AUM	Assets Under Management
CAB	Criminal Assets Bureau
CASP	Crypto-Asset Service Provider
CCF	Common Contractual Funds
CDD	Customer Due Diligence
CEA	Corporate Enforcement Authority
CFT	Countering the Financing of Terrorism
CFV	Central Register of Beneficial Ownership for Certain Financial Vehicles
CJA	Criminal Justice (Money Laundering and Terrorist Financing) Act 2010
CLG	Companies Limited by Guarantee
CPF	Counter Proliferation Financing
CRA	Charities Regulatory Authority
CRBOT	Central Register of Beneficial Ownership of Trusts
CSO	Central Statistics Office
DAB	Designated Accountancy Bodies
DAC	Designated Activity Company
DNFBP	Designated Non-Financial Businesses and Professions
DeFi	Decentralised Finance
DTA	Double Taxation Agreement
EBA	European Banking Authority
ECB	European Central Bank
EEA	European Economic Area
EEIG	European Economic Interest Groupings

Acronym	Full Form
EMI	Electronic Money Institution
ETF	Exchange-Traded Fund
EU	European Union
Europol	European Union Agency for Law Enforcement Cooperation
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
FMC	Fund Management Company
FSEC	Financial Sexual Extortion of Children
GDP	Gross Domestic Product
GNBCI	Garda National Bureau of Criminal Investigation
GNCCB	Garda National Cyber Crime Bureau
GNDOCB	Garda National Drugs and Organised Crime Bureau
GNECB	Garda National Economic Crime Bureau
GNI*	Modified Gross National Income (GNI*) at current market prices
GNIB	Garda National Immigration Bureau
GNPSB	Garda National Protective Services Bureau
GRAI	Gambling Regulatory Authority of Ireland
GRI	Greyhound Racing Ireland
HNWI	High-Net-Worth Individual
HPRA	Health Products Regulatory Authority
HRI	Horse Racing Ireland
HSE	Health Service Executive
HVG	High Value Goods
HVGD	High Value Goods Dealer
IBAN	International Bank Account Number
ICAV	Irish Collective Asset-Management Vehicle
ILP	Investment Limited Partnership
IMF	International Monetary Fund
INTERPOL	International Criminal Police Organisation
IVTS	Informal Value Transfer Systems
KYC	Know Your Customer
LEA	Law Enforcement Agency
LLP	Limited Liability Partnership
LP	Limited Partnership
LSP	Legal Services Provider
LSRA	Legal Services Regulatory Authority
LTD	Private Company Limited by Shares
MER	Mutual Evaluation Report
ML	Money Laundering

Acronym	Full Form
MLA	Mutual Legal Assistance
MLIU	Money Laundering Investigation Unit
ManCo	Management Company
MiCAR	Markets in Crypto-Assets Regulation
MiFID	Markets in Financial Instruments Directive
MoU	Memorandum of Understanding
NPO	Non-Profit Organisations
NRA	National Risk Assessment
NRB	Non-Retail Banks
OCG	Organised Crime Group
ODPP	Office of Director of Public Prosecutions
OECD	Organisation for Economic Cooperation and Development
P2P	Peer-to-Peer
PEP	Politically Exposed Person
PET	Privacy-Enhancing Technology
PF	Proliferation Financing
PI	Payment Institution
PLC	Public Limited Company
PMC	Private Members' Club
PMLN	Professional Money Laundering Network
POCA	Proceeds of Crime Act 1996
PPSN	Personal Public Service Number
PSRA	Property Services Regulatory Authority
RBO	Central Register of Beneficial Ownership of Companies and Industrial and Provident Societies
RCF	Retail Credit Firm
REQ	Risk Evaluation Questionnaire
SDU	Special Detective Unit
SEPA	Single Euro Payments Area
SNRA	Supranational Risk Assessment
SPE	Special Purpose Entity
SPV	Special Purpose Vehicle
STR	Suspicious Transaction Report
STReu	Suspicious Transaction Report with EU nexus
SoF	Source of Funds
TBML	Trade-Based Money Laundering
TBPF	Trade-Based Proliferation Financing
TBTF	Trade-Based Terrorist Financing
TCA	Trafficking for Criminal Activities

Acronym	Full Form
TCSP	Trust and Company Service Providers
TF	Terrorist Financing
TFS	Targeted Financial Sanctions
UCITS	Undertakings for Collective Investment in Transferable Securities
UN	United Nations
UNSCR	UN Security Council Resolution
VASP	Virtual Asset Service Provider
VAT	Value Added Tax
vIBAN	Virtual International Bank Account Number
WMD	Weapons of Mass Destruction

An Tánaiste's Foreword

As a highly globally integrated country, the security of both our society and wider economy are now more than ever inextricably linked and in turn represent the bedrock upon which our future progress and prosperity will be built. Protecting and nurturing these will create the conditions to allow us to provide for the future needs of our citizens. Equally, the integrity of our domestic and internationally-focussed financial system is non-negotiable.

We must also acknowledge that the very stability and sound legal frameworks that have made Ireland an attractive destination for people to live, work and invest here, also potentially makes us a target for those who seek to use these strengths for their own illicit ends. Money laundering, the financing of terrorism, and the proliferation of weapons of mass destruction erode the foundations of lawful commerce and public trust. They fuel organised crime, destabilise democracies, and in turn erode our national security. To protect our citizens, our international reputation, and play our part as a responsible EU member and global citizen, we must remain one step ahead of those who wish to exploit our openness.

This 2026 National Risk Assessment ("NRA"), developed by Ireland's Anti-Money Laundering Steering Committee ("AMLSC"), brings together the expertise of law enforcement, regulators, and the private sector. We have conducted a rigorous horizon scanning exercise to identify both persistent threats and emerging vulnerabilities. This document should not merely be a report; it is a roadmap. It provides the evidence-based foundation upon which the State will build more resilient Anti-Money Laundering and Countering the Financing of Terrorism frameworks.

Crucial to this effort are our gatekeepers: the businesses, banks, legal professionals, and accountants who serve as our first line of defence. This NRA provides these vital sectors with the tools and intelligence they need to maintain the ethical boundaries of our economy. As we look toward to our 2028 Mutual Evaluation Report, we are committed to a cycle of continuous improvement, ensuring a fresh NRA is produced every four years to meet evolving threats in this dynamic space.

Finally, we wish to extend our gratitude to the public servants, international partners, and civil society stakeholders whose collaboration made this work possible. We also wish to acknowledge Grant Thornton, who were commissioned to undertake the work that underpins

this report. Our task now is to move from assessment to action. By fortifying our system today, we ensure the security and prosperity of Ireland for the decades to come.

Simon Harris TD

Tánaiste and Minister for Finance

Foreword – Minister for Justice, Home Affairs and Migration

The strength and resilience of Ireland's financial system is central to Ireland's economic prosperity and national security. A strong financial sector, alongside designated non-financial businesses and professions, promotes employment and supports businesses and households across the country.

However, the openness and global connectivity that makes Ireland an attractive destination for trade and investment can also be exploited by criminals seeking to move and conceal illicit funds within the system. In addition, it can have broader implications for national security by facilitating the operations of organised crime groups and enabling them to plan and carry out harmful acts. This can erode confidence in the integrity of the economy, posing a risk to the safety and wellbeing of communities.

The National Risk Assessment recognises that the threat landscape is dynamic, adaptive, and increasingly complex. Criminal actors continuously exploit technological advancements and regulatory gaps to disguise illicit proceeds. For these reasons, it is crucial that the National Risk Assessment adopts a forward-looking, intelligence-led approach to identifying and assessing money laundering and terrorist financing threats, as well as the effectiveness of the enforcement frameworks designed to counter them.

At a strategic level, the National Risk Assessment highlights the evolving nature of predicate offences, the growing sophistication of financial crime networks, and the vulnerabilities within both traditional and emerging financial systems. It emphasises that risk is not static; it shifts in response to market developments, geopolitical pressures, and advancements in digital finance.

Equally critical is the evaluation of enforcement effectiveness. Strong legislative frameworks alone are insufficient without consistent oversight, intelligence sharing, and proportionate, dissuasive sanctions. Therefore, it is vital to assess not only the scale and nature of threats, but also the capacity of competent authorities to detect, investigate, and prosecute financial crime, as well as to recover criminal assets.

Ultimately, the National Risk Assessment serves as a cornerstone for a risk-based AML/CFT/CPF regime. The priority actions identified will inform policy priorities, guide

resource allocation, and strengthen national resilience against financial crime. By aligning threat assessment with enforcement capability, it will ensure that responses remain targeted, coordinated, and effective in safeguarding the integrity of our financial system.

Jim O'Callaghan TD

Minister for Justice, Home Affairs and Migration

Intentionally left blank

Executive Summary

The 2026 NRA is a central element of Ireland's ongoing efforts to counter Money Laundering, Terrorist Financing and Proliferation Financing ("ML/TF/PF"). This third iteration of the NRA delivers a comprehensive, national-level analysis of these risks, incorporating Ireland's first formal assessment of PF. This NRA draws on insights from across government departments, law enforcement and intelligence agencies, regulatory and supervisory bodies, industry groups and private sector stakeholders. It evaluates the threats and vulnerabilities that give rise to ML, TF, and PF, including the predicate offences that generate illicit proceeds.

This assessment provides the basis for informed policy development, enhanced risk-based supervision, and proportionate and effective measures across the public and private sectors, ensuring Ireland's frameworks are aligned with international standards and are responsive to evolving threats.

Key Findings

This NRA uses a four-tier risk rating scale: Low, Moderate, Significant and Very Significant.

ML Threats: The overall ML threat level in Ireland is rated as moderate. The highest threats are generated by drug offences and fraud, followed by theft and burglary, illicit trade and smuggling, human trafficking/exploitation and tax crime. While sanctions evasion has been assessed as low, continuing vigilance is warranted. Criminal networks are increasingly combining traditional cash-based methods with digital innovations such as crypto-assets, money mule networks, and complex layering techniques, making detection and disruption more challenging.

TF Threats: The TF threat is assessed as low, with risks arising from both domestic paramilitary groups and international terrorist networks. While the overall risk of a terrorist attack in Ireland remains low, the risk of TF activity - particularly small-scale, self-funded operations and the use of digital platforms - requires ongoing vigilance. The threat landscape is further complicated by the convergence of organised crime and terrorism, the emergence of right-wing extremism, and the growing use of online radicalisation and crypto-assets for fundraising and logistical support.

PF Threats: The PF threat is rated as low. This reflects Ireland's limited direct exposure to jurisdictions of PF concern. However, PF-related sanctions evasion requires continued vigilance, and indirect exposure to jurisdictions of concern through complex financial flows

and dual-use goods remains a risk. Ireland's status as an open economy means that vigilance is required to prevent the misuse of financial channels and trade structures for PF.

Sectoral Risks: ML risk in Traditional Retail Banks, Digital Banks, crypto-assets, e-money institutions, payment institutions which are money remitters and non-securitisation Special Purpose Entities ("SPEs") has been assessed as very significant, and TF risk in Traditional Retail Banks, Digital Banks, crypto-assets, and payment institutions which are money remitters has also been assessed as very significant. These heightened exposures stem from a variety of sources, including significant international linkages, the nature of the products and services available in the sector, and the scale and importance of the sectors in Ireland. From a PF perspective, all sectors have been assessed as low risk.

Although there is a high degree of consistency with the risks assessed in the previous NRA in 2019, the risk scores for some sectors have been updated, as listed in the table below. It should be noted that all the risk ratings in this report reflect a point-in-time assessment. Reflecting the dynamic factors which underpin these, they will continue to be monitored.

Sectors with Rating Changes Since the Previous NRA:

	2019 Risk Ratings	2026 Risk Ratings*
Investment Funds		
TF	Medium – High	Moderate
Funds Management Companies		
ML	Medium – Low	Significant
Funds Administrators		
TF	Medium – High	Moderate
Funds Depositories		
TF	Medium – High	Moderate
Crypto-Assets		
ML	Medium – High	Very Significant
TF	Medium – High	Very Significant
Bureaux de Change		
ML	High	Significant
TF	High	Moderate
Life Insurance		
TF	Medium – Low	Low
Legal Services		
TF	Medium – High	Moderate
Retail Bookmakers**		
TF	Medium – Low	Low
On-course Bookmakers**		
TF	Medium – Low	Low

Remote Bookmakers (Betting Intermediaries and Exchanges)**		
ML	Medium – Low	Significant
TF	Medium – Low	Low
Private Members' Clubs		
TF	Medium – High	Low
The Tote (both Horse Racing Ireland and Greyhound Racing Ireland)		
ML	Medium – Low	Low
TF	Medium – Low	Low
Express Trusts – Charitable Trusts		
ML	Medium – Low	Low
Companies		
TF	Medium – High	Moderate
Trust and Company Service Providers Supervised by Central Bank***		
ML	Medium – Low	Low
Non-Profit Organisations		
ML	Medium – Low	Low

**The 2026 rating scale (Low, Moderate, Significant, Very Significant) replaces the 2019 scale of Low, Medium-Low, Medium-High and High. For reference, Medium-Low corresponds to Moderate, Medium-High corresponds to Significant, and High corresponds to Very Significant.*

***This rating was assigned in 2018 as part of a sectoral risk assessment, apart from PMCs which were assessed in the 2019 NRA.*

****This rating was assigned in 2022 as part of a sectoral risk assessment on the Trust and Company Service Providers.*

Priority Actions

The NRA outlines a set of five high-level priority actions designed to strengthen Ireland's response to ML, TF, and PF risks. These focus on closing identified gaps and reinforcing measures already in place.

Risk and Coordination:

Identify emerging risks and challenges through collaboration with civil society to enhance understanding of the modus operandi of crimes and to support analysis. This will also include communication between Law Enforcement Agencies and prosecutors to discuss case-specific challenges while promoting mutual awareness and trust. This will be supported by multiple government agencies, including law enforcement, regulators, and legal entities, working together to identify and combat money laundering threats and will include the production of strategic analysis. This collaboration will ensure that all relevant parties share information, understand their roles, and align on strategies to effectively mitigate the risks identified in the NRA.

Capacity Building and Public Awareness:

Strengthen the AML, CFT, and CPF capacity of Law Enforcement Agencies, prosecutors, FIU Ireland, supervisors and reporting institutions through training and workshops. The focus will be centred on deepening the understanding of emerging risks and the modus operandi of ML, TF, PF. In addition, public awareness and education initiatives on mule accounts targeting vulnerable groups will be prioritised to ensure public vigilance.

Law Enforcement:

Strengthen risk-based, intelligence-led enforcement and enhance inter-agency and cross-sectoral co-ordination.

Framework (including Legal), Policy and Strategy:

Inform AML, CFT, and CPF measures with data and findings from the NRA. Policies, allocation of resources, and implementation of new, risk-based measures will be based on a comprehensive understanding of Ireland's specific ML/TF/PF threats and vulnerabilities.

Regulatory and Preventive:

This includes sectoral, entity-level risk understanding, supervision, regulatory actions (including enforcement), compliance obligations, outreach and information.

Introduction

This is Ireland's third NRA. It provides a consolidated, national-level analysis of ML, TF, and PF risks, and includes Ireland's first formal risk assessment of PF. This document updates and builds on all previous NRA documents, including the 2019 NRA, and the sector-specific risk assessments conducted since, and is based on the most up-to-date data and information available.[1]

Purpose

The purpose of Ireland's NRA is to systematically identify, assess, and develop a shared understanding of Ireland's ML, TF, and PF risks. This process is an essential component in ensuring that Ireland effectively and proportionately implements its AML/CFT/CPF legal, regulatory and enforcement frameworks, which are aligned with international standards, and support the integrity of the national and international financial system. A comprehensive NRA also provides valuable information to those working in sectors exposed to these risks.

Scope

This NRA provides a comprehensive, national-level analysis of ML, TF, and PF risks in Ireland.

- **Money Laundering** is the process of disguising the origins of criminal proceeds to make them appear legitimate. Under Irish law, any criminal offence which produces criminal proceeds can serve as a predicate for money laundering.
- **Terrorist Financing** involves providing or collecting funds, directly or indirectly, with the intention or knowledge that they will be used to carry out a terrorist act. This can involve both illicit and legitimate sources of funds.
- **Proliferation Financing** is the provision or movement of funds or assets to support the proliferation of Weapons of Mass Destruction ("WMD"), including related materials and delivery systems. For the purposes of this NRA, the focus is on the risk of breaching or evading proliferation financing related targeted financial sanctions, as well as broader risks linked to dual-use goods.

[1] The analysis undertaken in this Report was finalised in December 2025. Data or analysis published after this date has therefore not been incorporated. Where more up-to-date date becomes available, targeted update may be considered.

The sectors subjected to an in-depth sectoral risk assessment were drawn from the financial services and non-financial services sectors and were selected by the AMLSC. The ML, TF, and PF threats assessed are those which have been identified as the primary threats facing Ireland.

This assessment has been conducted to align with the internationally recognised standards set out by the Financial Action Task Force ("FATF"), European Union ("EU"), International Monetary Fund ("IMF"), World Bank and others. It was also conducted in a manner fully aligned to the specifics of Ireland's context, including the threat landscape.

The NRA evaluates both domestic and cross-border threats and vulnerabilities. This involved extensive engagement with government departments, law enforcement, regulatory and supervisory authorities, industry groups, regulated firms, and private sector stakeholders. The process is underpinned by a documented methodology approved by the AMLSC, ensuring consistency with international best practices and a robust, evidence-based approach to risk identification and analysis.

Objectives

The NRA is designed to provide a reliable foundation for policy and decision-making by describing and analysing the nature and scale of ML, TF, and PF in Ireland. It aims to inform the development of legislative frameworks, enhance risk-based supervision, facilitate effective law enforcement activity, inform those operating in relevant sectors on how to adapt their controls, and enable the efficient allocation of resources to areas of greatest risk. The NRA also seeks to enhance the capacity of both public authorities and private sector entities to manage and mitigate risks, while ensuring Ireland meets its international obligations. Ultimately, the NRA supports continuous improvement in the national framework for combating financial crime, fostering resilience and adaptability in the face of evolving threats.

Methodology

This NRA has been developed in accordance with a documented methodology. The methodology aligns to requirements and guidance from relevant bodies on the production of NRAs, including those in the EU Money Laundering Directive, papers issued by the FATF, EU, IMF and World Bank, and practices adopted by peer jurisdictions. The detailed methodology is set out in a separate document and summarised below.

Key Concepts

The methodology describes the approach for identifying and analysing ML, TF, and PF threats, vulnerabilities and consequences, as well as combining these to score overall levels of risk.

- A 'threat' is a person, group or activity with the potential to cause harm to the state, society or the economy. ML, TF, and PF threats are assessed in this document and are scored on a scale as described in Table 1. ML threats from a range of predicate offences are scored individually, and an overall ML threat score (combining the ML threats to obtain an overall ML threat score) is applied to all sectors.

- A 'vulnerability' can be exploited by a threat or may support or facilitate its activities. Vulnerabilities could relate to the inherent features of a particular sector, product or service, which makes them attractive and feasible for ML, TF or PF purposes. Vulnerabilities may also relate to gaps in the mitigation frameworks, e.g. a weakness in law, regulation, supervision, or enforcement. Vulnerabilities are primarily assessed on a sectoral basis in this document within each financial services sectoral risk assessment and non-financial services sectoral risk assessment and are scored on a scale as described in Table 1.

- 'Consequence' refers to the harm or impact caused by ML, TF, or PF, including effects on financial systems, the economy, and society. Consequences can be domestic or international, short or long-term, and may affect communities, businesses, national interests, or the reputation of the financial sector. Consequences are scored as described in Table 1 and are primarily assessed on a sectoral basis within each financial services sectoral risk assessment and non-financial services sectoral risk assessment.

- A 'risk' is the ability of a threat to exploit the vulnerability of a sector for the purpose of ML, TF, or PF, and the impact of this occurring. In this way, the risk is a result of

combining the threat, vulnerability and the consequence. Risks are scored on a sectoral basis in this document.

Table 1: Threat, Vulnerability and Consequence scoring criteria

Criteria	Low	Moderate	Significant	Very Significant
Threat	Minimal illicit funds or resources are generated, with basic laundering methods used. Organised Criminal Gang ("OCG") involvement is limited or absent, and activity is easily disrupted.	A moderate level of illicit funds or resources is generated, with limited laundering or financing methods. Some involvement by OCGs or other actors exists, but their operations can be disrupted.	A substantial amount of illicit funds or resources is laundered or transferred using a range of methods. OCGs or other organised actors are actively involved but may be somewhat vulnerable to disruption.	A high volume of illicit funds or resources is generated, using diverse and sophisticated laundering or financing methods. OCGs or other organised actors are heavily involved and highly resilient to disruption.
Vulnerability	The sector has low inherent exposure to ML, TF, or PF risks.[2] Strong controls are in place, and any vulnerabilities are isolated, well-managed, and unlikely to be exploited.	The sector has moderate inherent exposure to ML, TF, or PF risks. Some identified control gaps or operational weaknesses exist. Vulnerabilities may be exploited but are generally manageable.	The sector has notable inherent exposure to ML, TF, or PF risks. Control gaps are more widespread, and vulnerabilities are actively exploited or present a significant risk of exploitation.	The sector has high inherent exposure to ML, TF, or PF risks. Controls are weak or ineffective, and vulnerabilities are systemic, persistent, and likely to be exploited by criminal actors.

[2] Inherent exposure refers to the level of vulnerability an entity, product, service, or transaction has to ML, TF, or PF risks before any mitigating controls are applied.

Consequence	Minimal or localised impact. No significant harm to populations, communities, business environment, or national / international interests. No reputational damage to the financial sector.	Noticeable impact on specific communities or sectors. May cause short-term disruption or reputational concern but limited in scope and duration.	Broad impact affecting national interests, business environments, or population groups. May result in medium- to long-term harm or reputational damage to the financial sector.	Severe impact with international ramifications. Includes long-term harm to societal stability, national / international interests, or major reputational damage to the financial sector.

**The 2026 rating scale (Low, Moderate, Significant, Very Significant) replaces the 2019 scale of Low, Medium-Low, Medium-High and High. For reference, Medium-Low corresponds to Moderate, Medium-High corresponds to Significant, and High corresponds to Very Significant).*

To calculate overall sectoral risk, the scores were weighted via formula (for ML, scores comprised 60% vulnerability, 30% threat and 10% consequence, and for TF and PF, scores were 55% vulnerability, 30% threat and 15% consequence). Members of the AMLSC applied expert judgement to review the resulting risk scores. Overrides were approved in the 7% of instances, where expert judgement varied with the formula-based assessment.

Data Sources

The assessment of underlying threats, vulnerabilities and consequences was informed through both quantitative and qualitative data, expert judgment and stakeholder engagement. This approach ensured a consistent, evidence-based framework aligned with international standards and tailored to Ireland's national context. Key sources for this data are listed below:

- Government Departments
- Law Enforcement Agencies
- AML/CFT Regulatory and Supervisory Bodies
- Industry Bodies
- Firms in the regulated and unregulated sectors (including, in some sectors, through the issuance of sector specific questionnaires)

- Publicly available information, including open-source intelligence (both domestic and international)
- Qualitative insights from stakeholder interviews
- Comparative analysis of NRAs from peer jurisdictions

Geographic, Economic and Political Overview

Geographic

Ireland has a population of 5.5 million, one land border with Northern Ireland and an extensive western coastline, which create vulnerabilities to cross-border criminality, maritime criminal activities and terrorist activities involving neighbouring jurisdictions. Law enforcement, the Naval Service and customs authorities actively patrol Ireland's land and sea borders, working closely with European and UK partners to combat these threats.

Economic

Ireland is an open economy, with a relatively substantial financial services sector, and has been a member of the European Union since 1973. Ireland's EU membership enables Irish businesses to transact freely within the EU's Single Market which has a population of around 450 million, with tariff-free movement of goods, freedom to provide services and free movement of capital. This access significantly boosts cross-border trade, facilitating firms to expand into other EU markets. Ireland is also home to the EU subsidiaries and branches of hundreds of US multinational companies, particularly in export-intensive sectors like technology and pharmaceuticals. These firms contribute significantly to employment, exports, and tax revenues.

In 2024, Irish Gross Domestic Product ("GDP") was estimated at €563 billion. However, Modified GNI (known as "GNI*"), a better measure of domestic economic activity, was estimated at €321 billion. The Irish economy is a highly globalised one, with exports of goods and services representing 144% of GDP in 2024. In 2024, the EU was Ireland's largest goods export market, with €88.4 billion of goods exports in 2024, followed by the US, accounting for €73.5 billion of exports. The highest category of exports were medical and pharmaceutical products worth €99.7 billion, which accounted for 45% of goods exports in the year. In 2024, Ireland exported €483 billion worth of services, with financial services accounting for €27 billion. Ireland is ranked globally as the third freest economy on the Index of Economic Freedom since 2022, demonstrating a consistently high level of economic resilience and prosperity.

Political

Ireland is a parliamentary representative democracy, where the President is the head of State, and the Taoiseach (Prime Minister) is the head of Government. While the country is

administratively divided into 31 local authorities, central government exercises most state functions.

The Irish Constitution establishes and describes the main institutions of the State:

- *The Legislature (or legislative branch)*

Legislative authority is vested in the Oireachtas, which comprises the President of Ireland and two Houses, namely Dáil Éireann (House of Representatives) and Seanad Éireann (Senate).

- *The Executive (or executive branch)*

Executive power is exercised by the Government, which is nominated by the Taoiseach and approved by the Dáil, then appointed by the President.

By statutory provision, a general election to Dáil Éireann must be held at least once every five years. By constitutional provision an election for the presidency must be held every seven years, and a president may not serve more than two terms.

Seanad Éireann is the upper house of the Oireachtas. Its membership is partly elected and partly nominated by the Taoiseach. While it does not have the power to veto legislation, it plays an important advisory and revising role in the legislative process.

- *The judiciary (or judicial branch)*

The judiciary is responsible for interpreting and applying the law to disputes and conflicts, reviewing the constitutionality of laws, and ensuring that the other branches act within their constitutional powers. The Supreme Court is the highest court in Ireland and the court of final appeal. Judges are independent of the Government and can only be removed through a resolution of both houses of the Oireachtas for misbehaviour or incapacity.

The Judicial Appointments Commission was established in January 2025 as an independent body responsible for selecting and recommending appointments to all judicial offices. Only those recommended by the Commission may be nominated for appointment by the Government.

AML/CFT/CPF Frameworks

Ireland has developed comprehensive and robust legal, judicial and supervisory frameworks based on international standards and EU law to combat ML, TF, and PF, including frameworks designed to meet Ireland's obligations as a member of the EU. These aim to prevent and detect the proceeds of crime being laundered via the financial system, as well as detecting and preventing the funding of terrorism and WMD proliferation.

International

Financial Action Task Force

Ireland's AML/CFT/CPF frameworks are grounded in international standards set by the FATF. Ireland joined the FATF in 1991, shortly after its establishment in 1989. The FATF is the leading international body for developing AML/CFT standards, which are codified in the FATF's 40 Recommendations, and are assessed through FATF mutual evaluation processes. These evaluations assess how effectively member countries implement measures to combat ML, TF, and PF.

The FATF Recommendations and the outcomes of Ireland's mutual evaluations have been important in driving ongoing improvements to the national AML/CFT/CPF regime. As of the 2022 follow-up review, Ireland is rated Compliant or Largely Compliant with 34 Recommendations and has demonstrated substantial or moderate effectiveness across all assessed outcomes. Ireland continues to ensure that its framework aligns to FATF standards, and that new guidance issued is considered in the ongoing development of the AML/CFT/CPF regime.

European Union Framework

The Irish AML/CFT regime implements the standards set out in EU law, which substantially incorporate the FATF Recommendations through a series of AML directives and regulations as detailed in the Domestic Legal and Institutional Framework section. The EU "AML Package" which entered into law in 2024 further harmonises the regulatory approach, expands the scope of the regulation to include crypto-asset and crowdfunding providers, and establishes the new EU AMLA for direct supervision of highest-risk entities from 2028. Ireland

is progressing with its implementation of the additional requirements stemming from this AML Package.[3]

International Monetary Fund

Ireland's AML/CFT frameworks are also shaped by regular reviews from the International Monetary Fund ("IMF"). The IMF conducts Financial Sector Assessment Programme ("FSAP") reviews of Ireland on a five-year cycle, including to assess the effectiveness of financial regulation and AML/CFT controls. The most recent FSAP, published in July 2022, highlighted Ireland's growing exposure as a financial centre to cross-border money laundering risks.

Implementation of EU and UN Sanctions Regimes in Ireland

As an EU Member State, Ireland implements sanctions adopted under the EU's Common Foreign and Security Policy ("CFSP"), which are given legal effect primarily through Article 215 of the Treaty on the Functioning of the European Union. These include financial restrictions, travel bans, and trade embargoes targeting individuals, entities, and states involved in terrorism, human rights violations, and other threats to international peace and security.

As a UN Member State, Ireland is legally obligated to implement all UN Security Council Resolutions ("UNSCRs"), including those related to the non-proliferation of WMD. However, under Irish law, UN sanctions are only enforced once adopted by the EU, as there is no direct mechanism for a unilateral sanctions implementation regime. Accordingly, there are currently approximately fifty EU sanctions packages in place, some of which are issued under UNSCR, and others being adopted autonomously by the EU.

Ireland enforces EU sanctions domestically through Statutory Instruments, with oversight from designated competent authorities including the Department of Foreign Affairs and Trade, the Department of Enterprise, Tourism and Employment, and the Central Bank of Ireland. To support coordinated implementation of sanctions, Ireland has established the Cross-Departmental International Sanctions Committee ("CDISC"), which is chaired by the Department of Foreign Affairs and Trade. The CDISC brings together all relevant Government departments and agencies involved in sanctions implementation and enforcement, to facilitate a consistent and effective approach across the public sector.

[3] The majority of these new requirements must be transposed in Irish law by July 2027.

Sanctions Against Russia and Belarus

As a result of the illegal annexation of Crimea, the EU imposed restrictive measures against Russia in March 2014. The EU significantly strengthened these sanctions following Russia's full-scale invasion of Ukraine in February 2022. This has significantly increased the number of designated individuals and entities, and introduced sweeping measures aimed at undermining Russia's economic base, cutting access to key technologies and markets, and sharply reducing its ability to finance and conduct military operations.[4] The EU also broadened its sanctions against Belarus due to its direct involvement in, and support for, Russia's actions against Ukraine. These are in addition to pre-existing sanctions on Belarus and include a wide range of financial, trade, and economic restrictions.

The introduction and subsequent escalation of EU sanctions in response to Russia's actions in Ukraine have had a profound and sustained impact on the financial crime compliance landscape. As of February 2026, the EU had adopted 20 packages of restrictive measures against Russia. These unprecedented measures have become a central and increasingly complex component of the EU's sanctions frameworks, and they continue to evolve in response to ongoing attempts to circumvent them.[5] The sectoral sanctions against Russia focus on key areas of the economy and are governed by Council Decision 2014/512/CFSP and Council Regulation (EU) No 833/2014. These include restrictive measures in relation to several key sectors, including finance, trade, energy, transport, technology and defence.

Non-Proliferation

As a member of a wide range of disarmament and non-proliferation treaties and conventions, Ireland has a responsibility to ensure that robust domestic controls are in place to prevent the proliferation of weapons of mass destruction and conventional weapons.

The international system for controlling the export of dual-use goods is underpinned by several multilateral non-proliferation regimes. These regimes operate through voluntary arrangements between participating states and are designed to enhance global security by limiting the spread of sensitive goods, technologies, and expertise. Each regime maintains control lists identifying items that present proliferation risks. These lists are subject to regular

[4] European Commission / Sanctions Adopted Following Russia's Military Aggression Against Ukraine / Available from: https://finance.ec.europa.eu/eu-and-world/sanctions-restrictive-measures/sanctions-adopted-following-russias-military-aggression-against-ukraine_en#overview-of-sanctions-in-place

[5] European Commission / Guidance for EU Operators: Implementing enhanced due diligence to shield against Russia sanctions circumvention / Available from: https://finance.ec.europa.eu/document/download/3c86c9a8-f09e-4092-ab8c-a9e678df1494_en?filename=guidance-eu-operators-russia-sanctions-circumvention_en.pdf

review and amendment by technical experts from participating countries in order to reflect technological developments and evolving geopolitical conditions.

Ireland actively participates in all major international export control regimes and is represented in these fora by the Department of Foreign Affairs and Trade. Through participation in these frameworks, states agree to exercise controls over the import, export, transfer, and transit of specified goods and technologies. The export control regimes provide common guidelines and agreed control lists that participating countries, including Ireland, commit to implementing through their national export control systems.

Ireland is a member of the following principal international export control regimes:

- The Australia Group, which seeks to prevent the proliferation of chemical and biological weapons through coordinated export controls.
- The Missile Technology Control Regime, which focuses on controlling missile systems, components, and technologies, including those related to unmanned aerial vehicles.
- The Nuclear Suppliers Group, which aims to prevent nuclear proliferation by regulating the export of nuclear materials, equipment, and related technologies.
- The Wassenaar Arrangement, which promotes transparency and responsibility in the transfer of conventional arms and dual-use goods and technologies.

Together, these regimes provide a coherent and coordinated framework for non-proliferation controls, supporting consistent standards among participating states and reinforcing Ireland's approach to regulating sensitive items.

In addition, Ireland is party to a broad range of international arms control and disarmament agreements, including the Nuclear Non-Proliferation Treaty, the Treaty on the Prohibition of Nuclear Weapons, the Biological and Toxin Weapons Convention, the Chemical Weapons Convention, the Arms Trade Treaty, the Comprehensive Nuclear-Test-Ban Treaty.

Sanctions Against DPRK and Iran

The European Union's restrictive measures concerning the Democratic People's Republic of Korea ("DPRK") and Iran, as implemented in Ireland through national statutory instruments, form a core part of the State's obligations to counter the financing of weapons of mass destruction in line with FATF Recommendation 7. That Recommendation requires jurisdictions to implement targeted financial sanctions to prevent the proliferation of nuclear, chemical, and biological weapons, including by freezing assets without delay and prohibiting the availability of funds or financial services to designated persons and entities.

S.I. No. 148/2023, the European Union (Restrictive Measures concerning the Democratic People's Republic of Korea) Regulations 2023, provides for the enforcement of the targeted financial and trade measures contained in Council Regulation (EU) 2017/1509. This regime addresses the acute proliferation financing risks associated with the DPRK's nuclear and ballistic missile programmes and gives effect to the EU's obligations under relevant United Nations Security Council resolutions, which FATF Recommendation 7 expressly identifies as the basis for counter-proliferation financing measures.

The regulations require the freezing of funds and economic resources belonging to designated individuals and entities, together with prohibitions on making funds or economic resources available to them, whether directly or indirectly. These measures are central to the prevention of proliferation financing, as they cut off access to the financial system and prevent the mobilisation of resources for prohibited weapons programmes. The regime also prohibits certain activities related to military goods and technology, and imposes extensive export and import restrictions on dual-use items and other goods that could contribute to the DPRK's nuclear or weapons programmes. Transport restrictions, along with broad financial and investment sanctions, further reduce the risk that financial channels, logistics networks, or commercial structures could be exploited to support proliferation activities. An arms embargo remains in place, reinforcing the comprehensive nature of the counter-proliferation framework.

Similarly, S.I. No. 708/2023, the European Union (Restrictive Measures concerning Iran) (No. 4) Regulations 2023, implements EU restrictive measures that are expressly directed at the non-proliferation of weapons of mass destruction, and therefore at the risk of proliferation financing associated with Iran's nuclear and missile programmes. In line with FATF Recommendation 7, the regulations provide for the freezing of funds and economic resources of designated individuals and entities, and prohibit the provision of funds or economic resources to those listed. These obligations apply across the financial system and to all natural and legal persons, ensuring that no financial or economic support is made available to sanctioned actors.

The Iranian sanctions regime includes specific prohibitions on the provision of missile technology, addressing a key proliferation pathway. It also prohibits the satisfaction of claims arising from contracts or transactions affected by the sanctions, a measure designed to prevent the indirect release of frozen assets or the circumvention of restrictions through contractual enforcement. In addition, the regulations establish authorisation regimes for certain sensitive activities, including the provision of goods related to particular nuclear power activities and software designed for use in nuclear or military contexts. From a counter-proliferation financing perspective, these licensing and authorisation requirements

provide a controlled mechanism for scrutinising high-risk financial and commercial flows, rather than permitting unrestricted activity. An arms embargo remains in place in respect of Iran, further limiting the risk of material and financial support to military and proliferation-related programmes.

Taken together, these sanctions regimes demonstrate how Ireland gives effect to EU and UN-mandated targeted financial sanctions in accordance with FATF Recommendation 7. Through asset freezes, prohibitions on the availability of funds and economic resources, restrictions on financial and investment activity, and controls on high-risk goods, technology, and services, the measures ensure that the Irish financial system and wider economy cannot be used to finance or facilitate programmes involving weapons of mass destruction. A comprehensive and up-to-date list of the relevant statutory instruments is available on the Irish Statute Book, providing transparency and legal certainty for policy makers, regulators, financial institutions, and other designated persons with counter-proliferation financing obligations.

Domestic Legal and Institutional Framework

Ireland’s AML/CFT/CPF Legislative Frameworks

Ireland is a common law jurisdiction. Its legislative framework for combating ML and TF is primarily set out in the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, as amended (“CJA”) and in Part 4 of the Criminal Justice (Terrorist Offences) Act 2005 as amended. Ireland's national law implements successive EU directives and is consistent with international standards such as FATF recommendations. The CJA defines the offence of ML in terms of property which is the proceeds of criminal conduct. An ML offence is committed when 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, the State.

The CJA 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. Successive amendments to the Act have strengthened the legislative framework. Key actions taken include the following.

- The 2018 legislation, which transposed the EU 4th AML Directive. This update expanded definitions of Politically Exposed Persons ("PEPs") and beneficial ownership, and introduced mandatory business risk assessments.

- The 2021 legislation which transposed the EU 5th AML Directive. Key changes included the introduction of increased Customer Due Diligence ("CDD") measures. Particularly for PEPs, senior managing officials, and high-risk third countries. The definition of designated persons was expanded to include Virtual Asset Service Providers ("VASPs"), high-value art dealers, and certain letting agents.

- Ireland is working to align its national framework with the broader EU reform, which includes three key legislative instruments: the 6th AML Directive, which updates and strengthens national AML/CFT rules and will require transposition into Irish law; the AML-Regulation ("AMLR"), which establishes a harmonised "Single Rulebook" and is directly applicable across the EU; and the AML Authority Regulation ("AMLAR") which provides the new EU AML authority ("AMLA") with direct supervisory powers. This marks a significant shift from the previous Directive-led approach to a Regulation-led model, aiming for enhanced consistency across all member states. Most elements of the AML Regulation will apply from July 2027 and most elements of the Directive require transposition into national law by that date.

Ireland currently operates a dual reporting framework, in which all designated persons must report suspicious activity to both the Financial Intelligence Unit ("FIU") Ireland and the Office of the Revenue Commissioners ("Revenue"), who are responsible for investigating tax evasion. This will be changed as part of the updates required for the implementation of the 6th AML Package, with FIU Ireland being the single entity responsible for the receipt, analysis and dissemination of information contained in STRs in Ireland.

With respect to proceeds of crime, the relevant legislation is the Criminal Justice Act 1994 and the Proceeds of Crime Act 1996. These provide for both conviction-based asset seizure and civil asset forfeiture measures that do not require a criminal conviction, enforced by the Criminal Assets Bureau ("CAB").

The primary framework for TF is contained in Part 4 of the Criminal Justice (Terrorist Offences) Act 2005 which establishes the offence of financing terrorism and provides for the freezing and confiscation of funds used or intended for terrorist purposes.

Changes in Legislative Frameworks Since the Previous NRA

Since the 2019 NRA was published, there have been several amendments to the Irish legislative frameworks which are relevant to ML, TF, and PF including:

- The Solicitors (Money Laundering and Terrorist Financing) Regulations 2020 (S.I. No. 377 of 2020), introduced by the Law Society with the Legal Services Regulatory Authority ("LSRA"), replaced the 2016 Regulations to reflect updates from the Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018. While reinforcing solicitors' obligations under the AML regime, solicitors must continue to comply with the Act, maintaining effective policies and procedures to prevent and detect ML and TF. The Law Society is at an advanced stage in a process to introduce amending regulations (Solicitors (Money Laundering and Terrorist Financing) (Amendment) Regulations 2026) which will reinforce solicitors' obligations relating to amendments to the primary legislation in 2021, principally around beneficial ownership and enhanced due diligence. The timeline for introduction is Q2 2026.

- The EU's recent AML package includes a regulation which establishes a new EU wide Anti-Money Laundering Authority ("AMLA"); a regulation which introduces a harmonised "Single Rulebook" for designated persons; and a 6th AML Directive which sets out the obligations on Member States relating to supervision of AML obligations, FIU obligations, and the operation of Beneficial Owner and Bank Account Registers. This marks a significant shift from the previous directive-led approach to a regulation-led model, aiming for consistency across all Member States.

- The EU Instant Payments Regulation, entered into force in April 2024, amends and builds upon the Single Euro Payments Area ("SEPA") Regulation, and introduced mandatory requirements for instant credit transfers in euros. SEPA instant credit transfer allows the sending or receiving of euro-denominated payments within ten seconds for all payment service providers within SEPA. Instant payments can be made through all the channels that can be used to place non-instant credit transfers, such as online, in store and at a bank branch, and they can be made electronically at any time. The ability to receive SEPA instant credit transfers in euro became mandatory for euro area payment service

providers on 9 January 2025, and the ability to send these transfers became mandatory on 9 October 2025.

- Markets in Crypto-Assets Regulation ("MiCAR")
- European Union (Anti-Money Laundering: Beneficial Ownership of Corporate Entities) Regulations 2019 as set out in the Legal Persons and Arrangements section.

Upcoming Changes in Legislation

In addition, there are proposed changes to the Irish legislative framework which will, following enactment, enhance Ireland's AML/CFT frameworks.

- In 2025, the Proceeds of Crime and Related Matters Bill was introduced to update and strengthen Ireland's non-conviction based asset recovery and confiscation framework by enhancing the powers of the Criminal Assets Bureau and streamlining the procedures for freezing and recovering criminal assets. The Bill is currently progressing through the Houses of the Oireachtas.
- In June 2025, the Cabinet approved publication of the Criminal Justice (Terrorist Offences) (Amendment) Bill 2025, and the bill is currently making its way through the Houses of the Oireachtas. This legislative reform will strengthen Ireland's counter-terrorism framework, aligning domestic law with Directive (EU) 2017/541 on combating terrorism, and allowing for the prosecution of a broader range of terrorist and related financing activities. These include certain terrorist acts with a cross-border element, and cyber-attacks where the aim is to cause widespread harm. It would also facilitate Ireland's participation in enhanced counter-terrorism networks across the EU.

CAB and Revenue Confiscation and Forfeiture

The Criminal Assets Bureau ("CAB") recovers illicit funds through a combination of tax and social welfare enforcement powers and forfeitures and the disposal of assets determined by the courts to represent the proceeds of criminal conduct. The latter recoveries arise exclusively under the Proceeds of Crime Act 1996 (as amended), which provide for the freezing, seizure, and forfeiture of assets determined to be the proceeds of crime on a civil standard of proof. Following such actions, forfeited assets are typically liquidated and the funds generated are vested in the Minister for Public Expenditure, Infrastructure, Public

Service Reform and Digitalisation for the benefit of the Central Fund unless an injured party or victim of crime can be identified to the satisfaction of the Court.

Table 2: CAB funds returned to the Exchequer and other parties

Year	Exchequer	Other[6]	Total
2020	€4,293,743	€6,593,784	€10,887,528
2021	€5,549,661	€5,415,695	€10,965,357
2022	€6,337,668	€21,600	€6,359,268
2023	€8,651,396	€1,207,787	€9,859,183
2024	€17,052,458	€0	€17,052,458

Revenue officers (Customs) seize and detain cash under section 38 of the Criminal Justice Act 1994, with forfeiture to the Exchequer ordered by the Circuit Court under section 39 where the cash is proven, on the balance of probabilities, to represent the proceeds of crime or to be intended for use in criminal conduct.

Table 3: Revenue cash seizure and forfeiture order figures

Year	Cash Seizures	Seized Cash	Forfeiture Orders	Forfeited Cash
2020	66	€1,198,980	38	€1,013,180
2021	60	€1,079,290	36	€1,005,290
2022	55	€1,015,670	34	€1,012,670
2023	52	€1,045,320	30	€1,020,320
2024	49	€972,473	32	€1,106,677

Mutual Legal Assistance

Mutual Legal Assistance ("MLA") is the formal process through which Ireland cooperates with other jurisdictions in criminal investigations and proceedings. It facilitates the exchange of evidence and information, as well as providing for the freezing and confiscation of assets to support the administration of justice. The primary legislation governing MLA in Ireland is the Criminal Justice (Mutual Assistance) Act 2008, as amended. The Minister for Justice, Home Affairs and Migration acts as the Central Authority for MLAs and plays a key

[6] Amounts allocated to ODPP and/or victims/parties injured under POCA orders.

role in facilitating international cooperation by coordinating communication between competent authorities in Ireland and their counterparts abroad.

Table 4: Revenue and An Garda Síochána mutual legal assistance requests

	2020	2021	2022	2023	2024
Revenue					
Inbound	983	1,206	350	2,081	2,438
Outbound	502	361	139	362	456
An Garda Síochána					
Inbound	1,403	1,300	1,352	1,113	1,700
Outbound	286	561	754	660	672

Table 5: ODPP outbound mutual legal assistance requests (2020 – 2024)[7]

Jurisdiction	2020	2021	2022	2023	2024
EU Member States	241	287	264	404	322
United Kingdom	214	273	233	242	267
United States of America	266	378	338	271	360
Other	83	156	98	96	121
Total	**814**	**1,102**	**933**	**1,013**	**1,070**

Competent authorities for sanctions in Ireland

For each EU sanctions regime, the relevant Regulation requires Member States to designate National Competent Authorities ("NCAs"). In Ireland, the three competent authorities are: the Department of Foreign Affairs and Trade; the Department of Enterprise, Tourism and Employment; and the Central Bank of Ireland. Given the multi-sectoral nature of sanctions measures, a wide range of Government stakeholders are also engaged with sanctions-related issues.

Ministries and Coordinating Bodies

There are multiple Governmental bodies which play fundamental roles in developing and administering AML/CFT/CPF policy in Ireland. To ensure that these bodies work together effectively, Ireland has implemented several coordination frameworks.

[7] As a prosecutorial office the ODPP does not process inbound MLA requests.

Table 6: Government Departments (Ministries) and coordinating bodies

Committee / Forum	Description
Anti-Money Laundering Steering Committee ("AMLSC")	The AMLSC is a multi-agency committee formed in 2003, comprising of high-level officials from Standing and Associate members, consisting of regulatory bodies, governmental agencies, financial intelligence and law enforcement agencies, and chaired by the Department of Finance. The main purpose of the AMLSC is to provide a national, cross-sectoral forum for the oversight and active review of Ireland's AML/CFT frameworks. Also, where the Irish AML/CFT frameworks are to be presented to or considered by an external body (e.g., FATF, European Commission etc.) the AMLSC has responsibility for the facilitation, coordination and collaboration of such engagements.[8]
Cross-Departmental International Sanctions Committee ("CDISC")	The CDISC monitors, reviews, and coordinates the implementation, administration and exchange of information in respect of sanctions in Ireland. CDISC is chaired by the Department of Foreign Affairs and Trade, with the Department of Finance operating as Vice-Chair.
Private Sector Consultative Forum ("PSCF")	The PSCF is an AML/CFT information-sharing network comprising relevant public and private sector organisations. It brings together designated persons, competent authorities, and public agencies to facilitate discussion and information-sharing on AML/CFT matters, including financial crime prevention practices and processes, sanctions, and emerging threats and vulnerabilities.
Advisory Council against Economic Crime and Corruption ("ACECC")	The ACECC was established in 2022. It advises and makes proposals to Government on strategic and policy matters, and is responsible for developing a multi-annual strategy to combat economic crime and corruption.

Law Enforcement Authorities

Ireland has a single national police force, An Garda Síochána, which is responsible for carrying out all policing, security, and intelligence duties in the State. This practice is generally not observed in EU countries or internationally, but gives An Garda Síochána the benefit of consistency of approach, rapid sharing of information and intelligence between police and security units, and the ability to quickly redeploy resources to respond to changing needs and the benefits of economies of scope. An Garda Síochána also has the significant

[8] Terms of Reference – Ireland's Anti-Money Laundering Steering Committee / Available from: https://assets.gov.ie/static/documents/terms-of-reference-irelands-anti-money-laundering-steering-committee-may-2022.pdf

advantage of being the single point of contact with international counterparts. This enables an efficient contribution to the combating of international crime, including ML, TF, and PF.

An Garda Síochána is headed by the Garda Commissioner who is accountable to the Minister for Justice. The Minister is, in turn, accountable to the Dáil, the Irish legislature, in respect of policing and criminal justice matters. In 2025,[9] there were approximately 14,100 Garda in Ireland, who were supported by approximately 330[10] Garda Reserves and a further 3,650 civilian staff within An Garda Síochána.

While An Garda Síochána has a general responsibility for combating criminal conduct, including predicate offences that generate funds for laundering, certain branches of An Garda Síochána are particularly responsible for combating ML, TF, and PF.

Table 7: Branches within An Garda Síochána combating ML, TF, and PF

Branch Name	
Garda National Bureau of Criminal Investigation	
Garda National Cyber Crime Bureau	
Garda National Drugs and Organised Crime Bureau	
Garda National Economic Crime Bureau	FIU Ireland
	Money Laundering Investigation Unit
Garda National Immigration Bureau	
Garda National Protective Services Bureau	
Liaison & Protection	
Security & Intelligence	
Special Detective Unit	

In addition to these specialist units of An Garda Síochána, the combating of ML, TF, and PF in Ireland involves the close collaboration of the:

- CAB
- Revenue
- Office of the Director of Public Prosecution (“ODPP”)

[9] Garda HR Directorate / Available from: https://www.garda.ie/en/about-us/our-departments/human-resources-and-people-development/garda-hr-directorate/garda-and-garda-staff-numbers.html?
[10] Garda Reserve / Available from: https://www.garda.ie/en/careers/garda-reserve

Supervisory Framework

Ireland has several competent authorities for the AML/CFT supervision of Designated Persons, as defined under Section 60 of the CJA. Where a service or profession is not already regulated by a designated Competent Authority for AML/CFT purposes, supervisory responsibility falls to the Minister for Justice. The Minister may, by regulation, designate a Competent Authority for a specific class of Designated Persons.

Table 8: Competent Authorities for the AML supervision of Designated Persons

Competent Authority	Description
Central Bank of Ireland	The Central Bank of Ireland ("Central Bank") has a dual mandate as both a central bank and a regulator and supervisor of the financial sector. Along with prudential and consumer protection supervisory responsibilities, the Central Bank is the competent authority for AML/CFT supervision for credit and financial institutions in Ireland. The Central Bank adopts a risk-based approach to AML/CFT supervision, ensuring that credit and financial institutions ("Firms") receive supervisory oversight of their ML and TF frameworks appropriate to the level of risk posed by the Firm. The Central Bank issues guidelines, supervises its AML/CFT regulatory population, and may impose enforcement actions, with the aim of enhancing ML and TF risk mitigation in such Firms. The Central Bank actively promotes awareness of ML/TF risks posed to, and AML/CFT obligations on, the financial sector, including through the publication of guidance. In September 2019, the Central Bank issued its AML/CFT Guidelines for the Financial Sector which set out the Central Bank's expectations for Firms in complying with their AML/CFT obligations under Part 4 of the CJA, and subsequently updated these Guidelines in June 2021 following the transposition of 5AMLD into Irish law and other necessary amendments to clarify the internal governance obligations set out in the CJA. In addition to formal guidelines, the Central Bank issues 'Dear CEO' letters, circulars and press releases, and delivers speeches with additional insights for Firms, to highlight common deficiencies and provide insights to their regulatory priorities and expectations. Sectoral risk assessments of sectors under the AML/CFT supervision of the Central Bank have been conducted for the purposes of this risk assessment
Minister for Justice / Anti-Money Laundering Compliance Unit ("AMLCU")	The Minister for Justice is a state competent authority under the CJA and has delegated this function to the AMLCU under s.108 of the CJA. The AMLCU is responsible for supervising Designated Persons who are not otherwise overseen by another Competent Authority. These include High Value Goods Dealers ("HVGDs"); tax advisors not under other supervision;

Competent Authority	Description
	external accountants and bookkeepers who are not members of any Designated Accountancy Bodies ("DABs"); art traders and intermediaries involved in transactions of at least €10,000; notaries public not under other supervision; and Trust and Company Service Providers ("TCSPs") not supervised by the Central Bank or DABs. In addition, the AMLCU continues to be responsible for supervising gambling service providers including both retail and remote bookmakers, on-course bookmakers, and Private Members' Clubs ("PMCs") where gambling occurs, for AML/CFT compliance. These supervisory activities will transition to the Gambling Regulatory Authority of Ireland ("GRAI") once it is fully resourced to assume AML/CFT supervisory responsibilities. The AMLCU takes a risk-based approach to supervision of compliance with the CJA. Where instances of non-compliance are identified, the AMLCU will issue direction(s) to the Designated Person directing them to cease or refrain from engaging in certain actions until certain remedial actions are complete, or to undertake specific remedial actions to enhance their compliance programmes. The AMLCU released updated AML/CFT Guidelines for Designated Persons[11] in March 2024, to assist firms in relevant sectors understand their AML/CFT obligations and to set out regulatory expectations. Sectoral risk assessments of HVGDs, TCSPs, accounting services, and gambling have been conducted for the purposes of this risk assessment
Property Services Regulatory Authority ("PSRA")	The PSRA, established under the Property Services (Regulation) Act 2011, regulates and licenses Ireland's property services sector, covering auctioneers, estate agents, letting agents, and management agents. Its core functions include licensing and maintaining public registers such as the Residential Property Price Register and the Register of Licensed Property Services Providers. From an AML/CFT perspective, the PSRA monitors compliance levels and issues guidance, and where failures are identified it can issue administrative sanctions and can refer firms to law enforcement for serious breaches.
Gambling Regulatory Authority of Ireland ("GRAI")	The GRAI was established under the Gambling Regulation Act 2024, to regulate and license Ireland's gambling sector, covering betting, gaming, lotteries, and related services. The AMLCU will remain the competent authority for AML/CFT, pending the full establishment of the GRAI.

[11] Department of Justice, AMLCU Guidelines for Designated Persons / Available from: https://assets.gov.ie/static/documents/amltf-amlcu-guidelines-for-designated-persons.pdf

Competent Authority	Description
	Once operational, the GRAI will be the designated AML/CFT authority for the sector. Its enforcement powers will include issuing compliance notices, directing investigations, blocking online access, conducting hearings, and imposing administrative sanctions, including fines up to €20 million or 10% of turnover, and licence suspension or revocation.
Designated Accountancy Bodies ("DABs")	There are four DABs with statutory responsibility for AML/CFT supervision of firms offering services as an auditor, external accountant, tax adviser, or trust and company service provider. These are: Chartered Accountants Ireland – 27,581 members in Ireland with 1,722 member firms supervised in Ireland.[12] The Association of Chartered Certified Accountants – 13,179[13] members in Ireland with 584 member firms supervised in Ireland. The Chartered Institute of Management Accountants – 4,374 certified individuals and 54 members[14] who are subject to AML supervision. The Association of International Accountants – 242 members in Ireland with 30 member firms supervised in Ireland.[15] DABs are responsible for monitoring, inspecting, and enforcing compliance among their member firms. They can issue remediation directives for enhancing AML/CFT frameworks, impose disciplinary sanctions such as fines, suspension or expulsion of membership.
The Law Society of Ireland	The Law Society of Ireland is the statutory regulatory and professional body for solicitors in the State. It exercises statutory functions under the Solicitors Acts 1954–2015 in relation to the education, admission, enrolment, discipline, and regulation of the solicitors' profession. The society has 12,683 members.[16] It is also the competent authority for AML/CFT supervision for those solicitors offering services within the scope of the CJA. The Law Society monitors and assists compliance with the CJA through inspections and the provision of AML/CFT guidance and training to members. Enforcement powers include issuing directions, conducting practice inspections, referring breaches of AML/CFT legislation to the Legal Practitioners Disciplinary

[12] Chartered Accountants Ireland 2024 Annual Report, page 7
[13] Irish Auditing and Accounting Authority / Association of Chartered Certified Accountants / https://iaasa.ie/companies/aia/
[14] These members subject to AML supervision as they fall under Ireland's AML regulatory framework because they provide services that qualify them as "designated persons" under the CJA 2010.
[15] Irish Auditing and Accounting Authority / Association of International Accountants / https://iaasa.ie/companies/cipfa/
[16] Law Society of Ireland / Annual Report and Accounts 2024 / Available from: lsi-annual-report.pdf

Competent Authority	Description
	Tribunal and referring serious breaches to law enforcement or the Revenue Commissioners.
Legal Services Regulatory Authority ("LSRA")	The LSRA is the competent authority under the CJA for barristers acting as a "relevant independent legal professional", as defined in the CJA. The LSRA monitors AML/CFT practices, issues guidance, and can take enforcement actions such as mandating improvements or referring serious breaches to law enforcement. The authority has a roll of 3,071 practising barristers.

Table 9: Other Regulators Supporting the AML/CFT/CPF Frameworks

Regulator	Description
Charities Regulatory Authority ("CRA")	The CRA is responsible for maintaining public trust and confidence in the Irish charitable sector, by ensuring compliance with legal obligations, promoting good governance, and increasing transparency. It registers and monitors charities, publishes reports and data on key topics relevant to the sector, investigates concerns about their operations, and provides guidance to help regulated charities meet their responsibilities. The CRA also maintains a public register of charities, supports the development of the sector, and works to ensure that charitable resources are used exclusively for charitable purposes only as well as effectively for public benefit. The CRA has a statutory obligation, having consulted with An Garda Síochána, to remove from the register of charities, organisations which are promoting purposes which are in support of terrorism or terrorist activities.
Corporate Enforcement Authority ("CEA")	Established in July 2022 under the Companies (Corporate Enforcement Authority) Act 2021, the CEA derives its statutory mandate primarily from the Companies Act 2014. The CEA's responsibilities under the Companies Act 2014 include promoting compliance with company law, investigating suspected breaches, taking enforcement actions where necessary, supervising liquidators of insolvent companies, and managing a regime of restriction and disqualification undertakings for directors of insolvent companies. It also holds statutory functions concerning certain investment vehicles under the Irish Collective Asset-management Vehicle ("ICAV") Act 2015 and serves as the competent authority for imposing sanctions on company directors under the Companies (Statutory Audits) Act 2018.

Money Laundering Overview

This section presents the current understanding of the ML threat in Ireland, with a focus on predicate offences which generate illicit proceeds subsequently laundered into, out of, or through the country. The insights presented are informed by the collective expertise of Irish law enforcement agencies, the ODPP and other domestic and international partners. However, in common with the experience internationally, due to the inherently opaque nature of criminal activity, accurately quantifying the proceeds generated by different types of crime remains a challenge. As a result, this assessment is necessarily based on informed estimates and relevant expertise, rather than definitive figures. Estimates have been included in this assessment only where reliable primary sources could not be obtained.

The Money Laundering Process

Criminals typically launder money through a three-stage process:

1. **Placement:** Criminals attempt to launder money by depositing structured amounts into bank accounts to avoid detection, using cash to purchase high-value goods or services, or exploiting cash-intensive sectors such as hospitality and retail to place illicit funds into the legitimate economy.
2. **Layering:** Criminals obscure the origins of illicit funds through mechanisms such as transferring money across multiple accounts or jurisdictions, using shell companies, trusts, or professional intermediaries to create layers of complexity, or by investing in cryptocurrencies or other crypto-assets to exploit regulatory gaps and anonymity.
3. **Integration:** Illicit funds that have been successfully laundered are integrated into the economy through, for example, investment in real estate or legitimate businesses, the purchase of luxury goods and services, or the financing of further criminal enterprises to sustain and expand illegal operations.

Together, these stages form a process which enables criminals to benefit from illegal activities while minimising the risk of detection. Understanding this process is critical for regulators, law enforcement agencies, credit and financial institutions, and other sectors exposed to ML, including those assessed in the financial services sectoral risk assessments and the non-financial services sectoral risk assessments of this NRA. A clear grasp of how illicit funds move through and integrate into the legitimate economy enables these stakeholders to design and implement mechanisms to identify and investigate potential criminal activity.

Evolving and Emerging ML threats

The UNODC estimates that between 2% and 5% of global GDP is laundered each year. Against this backdrop, Ireland's position as a highly developed, open economy with domestic economic activity (known as GNI*) of €321 billion in 2024 and a sophisticated financial sector which creates an environment potentially conducive to ML. The country's integration into the EU Single Market, strong rule of law, and moderately outsized financial sector provide both opportunities and vulnerabilities for criminal actors seeking to exploit the legitimate economy for illicit purposes. The ML threat landscape in Ireland is shaped by both domestic and international factors, each presenting distinct but interconnected risks.

There is a significant shift in ML between traditional methods and digital innovation, and how money laundering is conducted across Europe. Traditional ML techniques remain widely used. For example, cash-intensive businesses are used to integrate illicit funds into the legitimate economy, physical cash couriers move money across borders, and young or vulnerable individuals are recruited as money mules. These methods persist because they are well-established, relatively simple, and effective within criminal networks. However, traditional methods are increasingly being complemented, and in some cases, replaced, by sophisticated digital methods that exploit regulatory gaps and cross-border vulnerabilities. Criminals now exploit crypto-assets for fast, borderless transactions, often layering funds through privacy-enhancing technologies. Techniques like chain hopping, switching between different crypto-assets, and the use of crypto-asset swapping services allow for greater anonymity, especially when operating in jurisdictions with weak AML oversight. Additionally, Decentralised Finance ("DeFi") platforms offer financial services without intermediaries, creating new opportunities for laundering outside traditional banking systems.[17]

The adoption of AI and digital onboarding has also introduced significant ML risks, as criminals exploit generative tools to automate ML schemes, conceal the origins of funds, and execute complex transactions that are more difficult to detect. Other methods can be leveraged to facilitate criminal activities, such as deepfakes, synthetic identities, and AI-generated documents – to bypass identity verification and automate fraud at scale. A 2024 FinCEN alert[18] highlights a surge in deepfake-related identity fraud targeting financial institutions, including the use of manipulated or entirely fabricated media to bypass due diligence processes and facilitate illicit financial activity. Intelligence from Irish law enforcement indicates that the expansion of remote onboarding has enabled the creation of

[17] Europol / The changing DNA of serious and organised crime / p.25 / Available from europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf
[18] Financial Crimes Enforcement Network, Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions / Available from https://www.fincen.gov/system/files/shared/FinCEN-Alert-DeepFakes-Alert508FINAL.pdf

large numbers of mule accounts, including accounts using manipulated or fabricated identity documentation, often from abroad. The international dimension, combined with falsified Irish addresses and synthetic or stolen identities, complicates detection and highlights the urgent need for enhanced cross-border cooperation, stricter onboarding controls, and real-time fraud detection systems tailored to evolving digital threats.

Domestic Risk

The primary ML threat in Ireland is from the proceeds of crime generated domestically, including drug trafficking, fraud, and other illicit activities. OCGs operating in Ireland – assessed further in the section on organised crime groups in Ireland of this document – are adept at exploiting both traditional and emerging technologies to launder illicit proceeds. The key feature of the domestic risk environment is the integration of criminal funds into the legitimate economy, most notably via real estate and other high-value assets. Criminals also make use of Irish financial and non-financial services providers, including banks, Credit Unions, payment institutions, crypto-asset service providers, and professional intermediaries such as solicitors and accountants, to place, layer and integrate illicit funds. While Ireland's regulatory and supervisory frameworks are robust and continue to evolve, the adaptability of domestic criminal networks and the convergence of traditional and digital methods mean that the domestic ML threat remains significant and requires ongoing vigilance and cross-agency cooperation.

International Risk

From an international perspective, Ireland's potential attractiveness to illicit actors is enhanced by its moderately outsized financial centre and its openness to trade and investment. Its strong rule of law can make it attractive to criminals, as it allows them to benefit from the legitimacy and stability associated with holding funds within the jurisdiction. As an international financial centre, Ireland has an inherent exposure to transnational ML threats. In recognition of this, a transnational financial flows assessment was undertaken as part of this NRA. Addressing these threats requires constant vigilance, strong regulatory frameworks, and close cooperation with international partners, as well as ongoing enhancements in data collection, analytics, and cross-border information sharing.

Money Laundering Prosecutions

The year-on-year increase in ML prosecutions in Ireland is largely attributable to heightened awareness and proactive efforts by both investigators and prosecutors. This has resulted in more prosecutions, whether for ML offences alone or in conjunction with other offences. Additionally, there has been a noticeable rise in the detection of ML offences, particularly

those involving 'money mule' activities. As the criminal justice system continues to strengthen its investigative and prosecutorial capabilities, criminal actors and their facilitators are adopting increasingly sophisticated laundering methods.

Table 10: Money Laundering Prosecutions (2020 – 2024)

Money Laundering Prosecution Statistics	2020	2021	2022	2023	2024
Prosecutions	344	548	605	729	831
Year-on-Year Increase in ML Prosecutions (%)	N/A	59%	10%	21%	14%

Money Laundering Predicate Offences

The predicate offences identified by Irish law enforcement agencies as posing the greatest ML threats in Ireland are assessed in this section. Other forms of revenue producing criminal activity, while not evaluated here, are not necessarily insignificant, and some which pose a lower ML threat may nonetheless cause substantial societal harm. Excluding these ML threats from this NRA aligns with the FATF definition of predicate offences and reflects the prioritisation of high-threat criminal activities under the European Multidisciplinary Platform Against Criminal Threats ("EMPACT") framework.[19]

Table 11: Overview of ML Predicate Offence threat ratings

Predicate Offence	Rating
Drugs	Significant
Fraud	Significant
Theft and Burglary	Moderate
Illicit Trade and Smuggling	Moderate
Human Trafficking and Exploitation	Moderate
Tax Evasion	Moderate
Cybercrime	Low
Financial Sanctions Evasion	Low
Bribery and Corruption	Low

Where relevant, this section also examines funds that are laundered in Ireland but originate from illicit activity abroad, as well as proceeds of crime committed in Ireland that are

[19] Europol / EU Policy Cycle – EMPACT / Available here: EU Policy Cycle - EMPACT - EMPACT 2022+ Fighting crime together | Europol

subsequently laundered internationally. This approach ensures a comprehensive understanding of Ireland's role in both domestic and international ML networks.

Taking account of the range of predicate offences and their relative severity, Ireland's overall ML threat is assessed as moderate. This assessment indicates a material level of ML risk, arising from a combination of domestic criminal activity and transnational laundering dynamics.

Drug Offences

Rating

Drug offences generate the largest volume of illicit funds in Ireland, with the final proceeds primarily being in cash. Ireland serves both as a destination and transit country for illegal drugs, with strong links between drug markets and domestic and international OCGs. The high volume of illicit funds generated by the drug trade necessitates a criminal infrastructure to facilitate laundering activities, and these groups systematically launder proceeds through complex financial channels, including extensive bank account networks, Informal Value Transfer Systems (''IVTS''), crypto-assets, and lifestyle-based laundering methods. As a result, drug offences are assessed as posing a significant ML threat.

Overview

The EU retail drug market is estimated to be worth over €30 billion annually, making it one of the most lucrative criminal activities in Europe. Europe also shows the highest rates of people arrested, prosecuted, and convicted for drug trafficking and use or possession per 100,000 population.[20] This immense scale reflects high levels of drug availability and demand, with Europe serving as both a major consumer base and a key hub for global drug trafficking. Around 83.4 million or 29% of adults (aged 15-64) in the EU are estimated to have used illegal drugs at least once in their lifetime.[21]

Ireland is both a destination for drugs produced overseas, as well as a transit route for onward distribution to nearby larger markets, including the UK and mainland Europe. Ireland has over 3,000 kilometres of coastline, and this, combined with its strategic Atlantic position makes Ireland an ideal entry point and transit route for international drug smuggling operations. While Ireland is not generally a drug production country, there is evidence that limited amounts of cannabis are grown domestically.

Given the high value of the illicit drug market and the substantial criminal proceeds it generates, offenders exploit a broad range of ML typologies to conceal the origin of these funds and integrate them into the legitimate economy. In Ireland, drug sales to end users are

[20] UNODC World Drug Report / Available from: https://www.unodc.org/documents/data-and-analysis/WDR_2024/WDR_2024_SPI.pdf / p.16
[21] Health Research Board – European Drug Report 2024 / Available from: https://www.hrb.ie/press-releases/european-drug-report-2024/?utm

predominantly cash-based, and cash-based ML typologies are therefore particularly relevant at the initial placement stage of ML.

Drug Production and Use

Cannabis is the only illegal drug known to be produced in Ireland. It remains the most used illegal drug in the country, with 91% of those who have used drugs within the last 12 months having used cannabis.[22] While there has been a shift towards homegrown cannabis, significant amounts of foreign-produced cannabis products are still seized by authorities. Current evidence suggests that synthetic drug production within Ireland is limited, and most seizures of synthetic drugs have originated from foreign jurisdictions. However, Ireland could start to see the emergence of local synthetic drug manufacturing, as the raw materials required for production become more available. Other European countries – including Belgium and the Netherlands – have significant domestic production capabilities.

Based on the Healthy Ireland Survey 2023,[23] 7.3% of adults reported using illicit drugs in the past year, with cannabis being the most used (6.1%), followed by cocaine (2%), ecstasy (0.8%), magic mushrooms (0.8%), and ketamine (0.4%). While overall drug use levels remained stable compared to 2019–20 (7.4%), there were slight increases in cannabis and cocaine use, and a notable decline in ecstasy use from 2.2% to 0.8%. Additionally, 7% of respondents reported using sedatives without a prescription. These trends reflect evolving patterns in drug consumption across Ireland.

Drug Transit Through Ireland

Ireland is a known maritime transit point for cocaine and other drug shipments destined for the UK and mainland Europe, often entering via routes from Latin America.[24] These routes are exploited by transnational OCGs using both commercial and private vessels. The increase in maritime activity is consistent with patterns observed across all European countries with a coastline since 2022. See Table 12 for recent examples of drug seizures involving Ireland, which illustrate the country's exposure to international trafficking networks and the diversity of source countries and smuggling methods. While it is difficult to quantify the total value of drugs transited through Ireland, high-profile cases, such as the €157 million

[22] Health Research Board / Focal Point Ireland: National Report for 2024 – Drugs / Available from: https://www.euda.europa.eu/system/files/documents/2025-06/national_report_ireland_2024_drugs.pdf?utm_source=copilot.com / p.8
[23] Health Research Board / Findings from the Healthy Ireland Survey / Available from: https://www.hrb.ie/wp-content/uploads/2025/07/Findings-from-the-Healthy-Ireland-Survey-FINAL.pdf / page 6
[24] The Azure Forum / Ireland's place in the global cocaine trade and implications for public security / 2023 / Available from: https://azureforum.org/irelands-place-in-the-global-cocaine-trade-and-implications-for-public-security /

cocaine seizure aboard the MV Matthew, highlight the scale of these operations and their links to transnational OCGs.

Drug Seizures

Since the publication of Ireland's 2019 National Risk Assessment, where drug seizures were valued at €23.6 million, there has been a sharp escalation in interdiction outcomes. For 2024, the estimated value of drugs seized had reached €214.7 million, a ninefold increase, reflecting both the growing volume of drugs trafficked into and through Ireland and the success of targeted enforcement strategies by An Garda Síochána, Revenue, and international partners.

Figure 1: Value of drug seizures (2020 – 2024)[25]

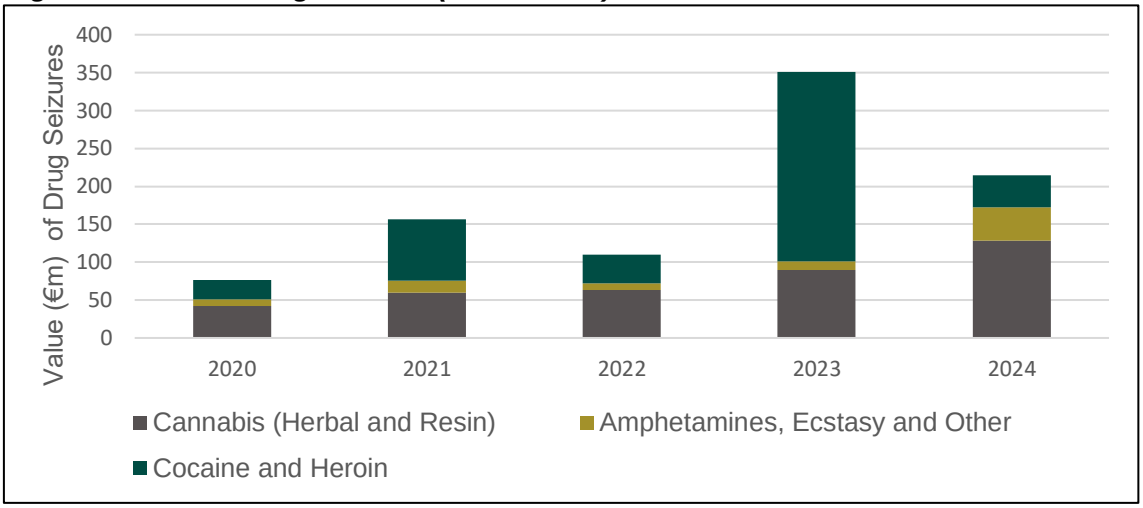


Table 12: Recent significant drug seizures

Origin	Details
South America	The September 2023 MV Matthew operation, seizing 2.3 tonnes of cocaine valued at over €157 million, demonstrates the magnitude of drug trafficking occurring in and through Ireland. While the shipment was primarily intended for onward distribution to the UK and mainland Europe, its interception highlights Ireland's strategic role in transnational trafficking routes and the capacity of Irish OCGs to move large volumes of illicit drugs through Irish territory.
	In July 2025, Irish authorities seized 440kg of cocaine following a coordinated maritime interdiction operation off the coast of Cork, Ireland.
Canada	In December 2023, 300kg of cocaine valued at €21 million was intercepted on a Maltese-registered cargo vessel arriving from

[25] Ibid.

	Canada at the Port of Foynes, County Limerick. Additionally, in October 2023, 186kg of herbal cannabis worth €3.7 million was seized at Dublin Airport, having arrived in air cargo consignments from Canada.[26]
Netherlands	In November 2023, Revenue officers in Athlone seized 2kg of ketamine, 313 grams of MDMA tablets, 118 grams of MDMA powder, and 31 grams of cocaine, all originating from the Netherlands and destined for Dublin.[27]
	In May 2025, Revenue officers at Dublin Port seized 20kg of heroin and 37kg of cocaine, with an estimated value of €5.4 million. The shipment originated in the Netherlands and was destined for an address in County Cavan.[28]
Bulgaria	In October 2023, 13kg of cocaine was found concealed in a Bulgarian-registered cab unit at Rosslare Europort.[29]
United States	In 2024, authorities seized €35.5 million of herbal cannabis, amounting to 1,778kg, a 100% increase compared to 2023. Seizures of US-origin cannabis in Ireland have risen sharply, with a 700% increase since 2020. In 2023, authorities confiscated 834kg of cannabis valued at €16.6 million.[30]
Germany	In November 2023, Revenue officers seized 210kg of herbal cannabis with an estimated value of €4.2 million at Dublin Port.[31]
Australia (transit)	In February 2024, authorities seized over half a tonne of methamphetamines worth €32.8 million, concealed in industrial machinery shipped from Cork Port to Australia with links to Mexican cartels.[32]

Law Enforcement Intelligence

Ireland continues to face a significant and evolving threat from OCGs involved in drug trafficking, with cocaine remaining the most prevalent substance. Synthetic drugs are an emerging concern, with production hubs in mainland Europe, and Ireland is increasingly both a country of transit and an end-use market. OCGs involved in drug trafficking operate with

[26] An Garda Síochána / Revenue seize cocaine worth €21 million in Limerick / https://www.garda.ie/en/about-us/our-departments/office-of-corporate-communications/press-releases/2023/december/revenue-seize-cocaine-worth-21-million-in-limerick.html?utm
[27] Revenue / Revenue seize drugs work over €4.6 million in Dublin and Athlone / https://www.revenue.ie/en/corporate/press-office/press-releases/2023/pr-110323-drugs-dublin-athlone.aspx?utm
[28] Revenue / Revenue seize drugs worth €5.4 million in Meath / https://www.revenue.ie/en/corporate/press-office/press-releases/2025/pr-052825-meath-drugs.aspx
[29] Revenue / Revenue seize cocaine and cash worth almost €389,000 at Rosslare Europort / https://www.revenue.ie/en/corporate/press-office/press-releases/2023/pr-102823-cocaine-cash-rosslare.aspx?utm
[30] The Times / How the United States became a major supplier of weed to Ireland / https://www.thetimes.com/world/ireland-world/article/united-states-is-major-supplier-of-weed-to-ireland-nc7t3hmb8?utm
[31] Revenue / Revenue seize drugs worth over €4.6 million in Dublin and Athlone / https://www.revenue.ie/en/corporate/press-office/press-releases/2023/pr-110323-drugs-dublin-athlone.aspx?utm
[32] Irish Independent / Two Kerry men in custody following crystal meth haul appear in court again / https://www.independent.ie/regionals/kerry/news/two-kerry-men-in-custody-following-crystal-meth-haul-appear-in-court-again/a2140941957.html

corporate-like structures and exploit border vulnerabilities to maintain transnational networks and utilise a wide range of techniques to launder proceeds.

Fraud

Rating

Fraud generates substantial illicit proceeds in Ireland through increasingly complex and high-value schemes such as investment scams, VAT carousel operations, and cyber-enabled fraud. These often involve transnational actors and sophisticated laundering techniques, including mule networks, shell companies, and crypto-asset conversions. While not always linked to traditional OCGs, many fraud operations are run by highly resilient and technically skilled networks that exploit digital infrastructure and adapt quickly. The scale, complexity, and cross-border nature of these activities, coupled with their reliance on sophisticated laundering techniques, significantly elevate the risk profile. Consequently, fraud-related offences are assessed as posing a significant ML threat.

Overview

In Ireland, fraud offences encompass a broad spectrum of criminal activities, which An Garda Síochána categorises into 20 sub-types. The four categories shown in the table below are the most common, accounting for 7,510 cases – approximately 66% of the 11,431 fraud incidents reported to An Garda Síochána in 2024.

Table 13: Highest number of incidents recorded (2019 vs 2024)[33]

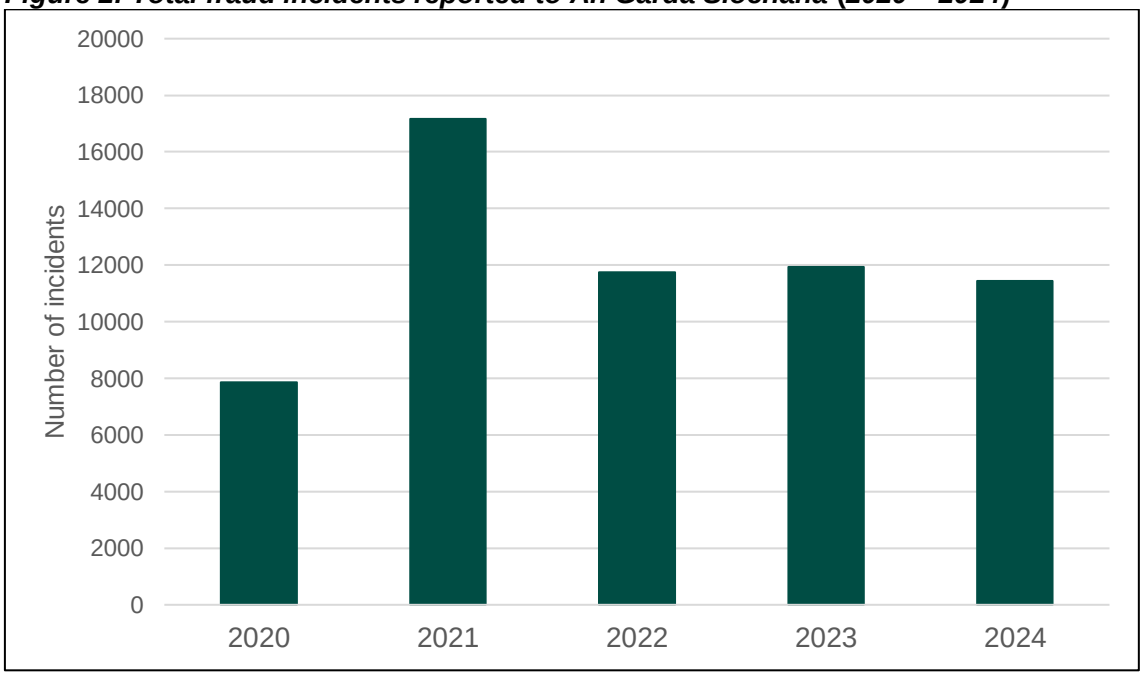
Fraud Type	Incidents (2019)	Incidents (2024)	% Change
Fraud, Deception and Related Offences	3,024	3,498	+16%
Phishing/ Vishing/ Smishing Fraud	313	2,069	+561%
Account Takeover Fraud	355	1,137	+220%
Shopping/ Online Auction Fraud	402	806	+100%

As most fraud is perpetrated through digital means, a primary objective for criminals is to rapidly move illicit funds beyond the reach of authorities and the regulated financial system. In this context, crypto-assets and IVTS are particularly attractive, offering the potential for anonymity, international transfer, speed, the ability to bypass traditional financial controls, and an enhanced opportunity to evade tracing and recovery efforts.

[33] In December 2024 and March 2025, the CSO highlighted a backlog in recording fraud-related incidents reported by financial institutions under Section 19 of the Criminal Justice Act, 2011. The CSO have continued to publish fraud statistics based on the public reports recorded, the figures should be interpreted with caution, as they are incomplete and may understate the true scale of such offences / Available here: https://www.cso.ie/en/releasesandpublications/ep/p-rc/recordedcrimeq12025/keyfindings/

Figure 2 below illustrates the trend in reported fraud incidents. An Garda Síochána notes that fraud levels remained stable prior to a sharp increase during the COVID-19 pandemic, largely driven by the widespread shift to online activity, which created more opportunities for cyber-enabled fraud. Although levels have since declined, they remain elevated compared to pre-pandemic norms, with recent years showing a consistent volume of reported incidents. Irish law enforcement has seen significant progress in targeting fraud. Between 2020 and 2022, arrests related to fraud offences increased from 232 to 402, a rise of 73%.[34]

Figure 2: Total fraud incidents reported to An Garda Síochána (2020 – 2024)[35]



Based on current fraud trends, key threats include:

Cyber-Enabled Fraud: Cyber-enabled fraud typically involves fraudulent activity conducted in the cyber environment and involves two key elements: (i) cross-border criminality, involving international actors and the movement of illicit funds, and (ii) manipulative social engineering techniques aimed at deceiving individuals into disclosing sensitive or personal information. Cyber-enabled fraud along with related ML, is often orchestrated by transnational OCGs.[36]

[34] Available from: https://www.oireachtas.ie/en/debates/question/2022-11-29/section/490/ (Data originally provided to Minister for Justice based upon operational data from An Garda Síochána's PULSE system).
[35] Available from: https://www.oireachtas.ie/en/debates/question/2022-11-29/section/490/? (Data originally provided to Minister for Justice based upon operational data from An Garda Síochána's PULSE system)
[36] FATF, Interpol, Egmont Group / Illicit Financial Flows from Cyber-Enabled Fraud / Available from: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Illicit-financial-flows-cyber-enabled-fraud.pdf.coredownload.inline.pdf

Account takeover fraud, phishing/vishing/smishing fraud, and card not present fraud are all examples of cyber-enabled fraud, and as noted in (Table 13) have all increased in recent years.

The ongoing growth and adoption of digital technologies have been significant factors in the rise of cyber-enabled fraud. The location where cyber-enabled fraud takes place, typically where the victim resides, is often separate from where the proceeds are laundered. Intelligence suggests that jurisdictions with advanced digital financial systems, where most transactions occur online, are especially vulnerable to cyber-related ML risks. Nonetheless, the cross-border nature of this crime enables perpetrators to exploit victims globally with relative ease.

Case Study: International Cyber-Enabled Fraud Investigation

Ireland, through the Garda National Economic Crime Bureau ("GNECB"), played a pivotal role in an INTERPOL-led global investigation targeting the 'Black Axe' organised crime group, a West African-originating network involved in Business Email Compromise ("BEC") and Romance Fraud. The operation was triggered by a Europol request following a €1.1 million BEC fraud, with funds laundered through Asia. The investigation revealed that Ireland was not only a conduit for laundering proceeds (primarily via the use of Irish bank accounts), but also a base of operations for elements of the gang.

Several BEC-related cases have been investigated as part of operations in Ireland that resulted in asset recovery:

1. A company reported the theft of over €98,000 in a BEC fraud, transferred to a Portuguese bank account. Due to swift action, the transaction was cancelled, and the full amount recovered.
2. A victim purchasing property in Spain lost over €149,000 in a BEC scam. GNECB, working with the relevant financial institution, recovered nearly €76,000 from a secondary Spanish bank account.
3. Over €95,000 was stolen from a U.S.-based victim in April 2023 and laundered through an Irish bank account. GNECB froze the funds and successfully recovered over €91,000.

In total, across seven cases involving Irish companies, more than €475,000 was stolen, of which over €400,000 was successfully recovered.

Fraudulent Payments: Fraudulent payments cover a variety of fraud types (e.g. phishing, manipulation of payer, or making unauthorised payments using lost or stolen cards)

committed on all payment types (e.g. credit transfers, card payments, e-money, and direct debits).[37] Payment fraud is an increasing threat in Ireland. The total value of fraudulent payments[38] for Irish resident payment service providers[39] rose to €160 million in 2024 from €129 million in 2023 and €102 million in 2022; the number of fraudulent transactions[40] grew at a faster pace, more than doubling from 400,000 in 2022 to 815,000 in 2024.[41]

The fraud threat varies depending on the transaction type. In 2024:

- For card payments, 88% of the fraud by value was related to "issuance of payment order by fraudster" of which 68% related to card details theft and 23% to lost or stolen cards;
- For credit transfers, 46% involved manipulation of the payer,[42] and 54% the issuance of a payment order by the fraudster;
- For e-money, 56% involved manipulation of the payer, and 42% the issuance of a payment order by the fraudster.

Cross-border payments dominate fraud trends across all payment types except cheques and cash withdrawals; this trend is largely reflective of broader trends across the EU.[43]

Investment Fraud: Investment fraud can take different forms, however, it generally involves offering investment into a scheme which does not exist or one where the benefit is greatly exaggerated by fraudsters, with perpetrators often targeting victims remotely via online and social media platforms. There has been a significant increase in reported investment fraud in Ireland in recent years, with €14 million reported stolen in 2021, €11.5 million in 2022 and more than €25 million in 2023.[44] There has been a corresponding increase in the number of reported incidents; with 45 cases in 2019, rising to 176 in 2022, a 291% increase.[45] Common investment scams include shares, bonds, cryptocurrencies, pensions, and overseas land

[37] Central Bank of Ireland / Insights from Irish Payment Fraud Statistics / 2025 / Available from: https://www.centralbank.ie/statistics/statistical-publications/behind-the-data/insights-from-irish-payment-fraud-statistics
[38] Fraudulent payments, on the other hand, refer to the total monetary value of those fraudulent transactions. This gives insight into the financial impact of fraud, rather than just its frequency.
[39] Noting that many PI/EMI firms will service transactions with both origin and destination outside Ireland
[40] Fraudulent transactions refer to the number of individual payment events that have been identified as fraudulent. This metric counts each instance where fraud occurred, regardless of the amount involved.
[41] Central Bank of Ireland Payment Fraud Statistics 2024 https://www.centralbank.ie/statistics/data-and-analysis/payment-fraud-statistics
[42] Situations in which fraudsters gain trust by social engineering or impersonation, and convince the victim to make payments to them
[43] Central Bank of Ireland / Insights from Irish Payment Fraud Statistics / 2025/ Available from: https://www.centralbank.ie/statistics/statistical-publications/behind-the-data/insights-from-irish-payment-fraud-statistics
[44] An Garda Síochána / AGS report an over 90 per cent increase in investment fraud in 2023 / https://www.garda.ie/en/about-us/our-departments/office-of-corporate-communications/press-releases/2024/april/ags-report-an-over-90-per-cent-increase-in-investment-fraud-in-2023.html
[45] Central Statistics Office / PULSE Crime Database Data (Provided by Central Statistics Office)

investment; 44% of the reports to An Garda Síochána relating to investment fraud referenced ‘Bitcoin’ or ‘crypto’. This mirrors the picture in Europe, with Europol stating that investment fraud generates millions of euros of illicit profits, virtual assets remain reported as the product most offered to victims in this type of fraud.[46]

Law Enforcement Intelligence

The highest volume of fraud incidents currently falls under phishing, vishing, and smishing, which are executed primarily through digital and telecommunications channels, leveraging deceptive emails, texts, and calls to manipulate victims into revealing sensitive financial information or authorising transactions. These frauds result in funds being extracted from victims’ accounts and swiftly moved beyond the reach of authorities, often through digital payment platforms, money mules, and increasingly, crypto-assets.

[46] Europol / Internet organised crime threat assessment (IOCTA) / 2024 / Available from: https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf / p. 30

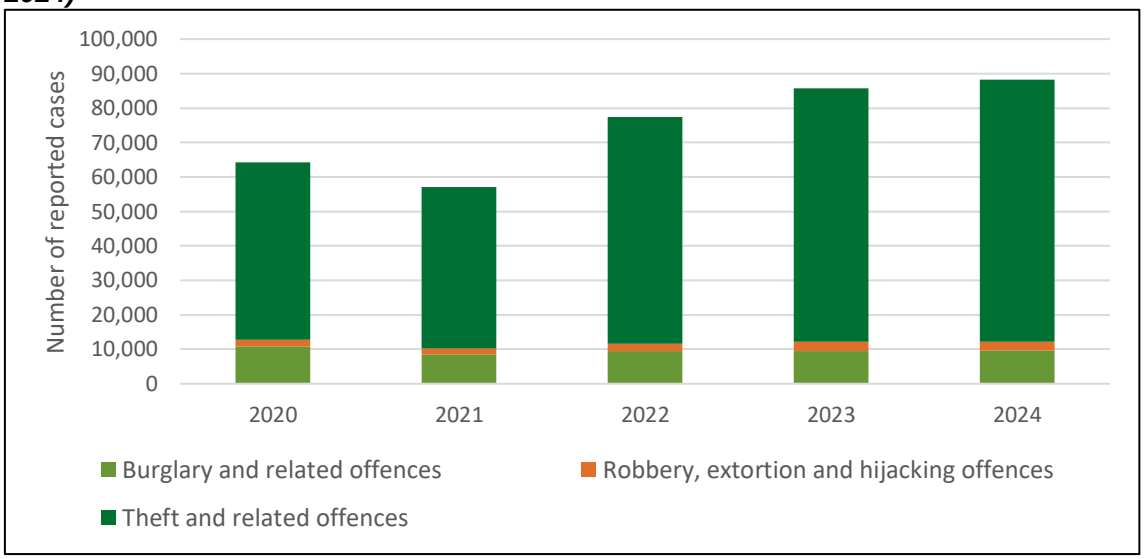
Theft and Burglary

Rating

Theft and burglary offences generate illicit proceeds primarily through domestic burglary gangs and organised armed robbery groups. While armed robberies are not frequent occurrences, they can produce significant proceeds for OCGs. Theft-related offences have risen modestly in recent years, whereas burglary rates have remained relatively stable. In relation to burglaries, most incidents involve low-value property crime, with a proportion being linked to OCGs. Although some high-value cases exist, including targeted robberies and the resale of stolen goods via informal and online channels, the overall volume of proceeds available for laundering remains limited. Accordingly, theft and burglary offences are assessed as posing a moderate ML threat.

Overview

Figure 3: Reported cases of burglary, robbery, extortion, hijacking and theft (2020 – 2024)[47]



The past decade has seen a sustained and significant fall in the number of burglaries and related offences, with 2024 reported figures 42% lower than in 2019. This has been driven by Garda initiatives targeting burglary through prevention and enforcement strategies. Robbery, extortion and hijacking offences have remained at consistent levels, although there was a decrease during 2020 and 2021, likely due to the COVID-19 pandemic. Theft and

[47] Central Statistics Office / https://ws.cso.ie/public/api.restful/PxStat.Data.Cube_API.ReadDataset/CJA01/XLSX/2007/en

related offences have trended upwards over the same period, rising by 12% between 2019 and 2024, albeit with significant declines in 2020 and 2021. This trend of property crime reducing during COVID-19 was also experienced across Europe, with reports[48] suggesting that this crime type shifted during the pandemic to target unoccupied commercial sites and trucks, and the targeting of medical and pharmaceutical products.

Across the EU, more than 1.2 million burglaries were reported in 2023, representing a 14% decrease from 1.4 million in 2019.[49] Stolen goods can be sold via second-hand shops, phone shops, jewellery shops, pawnshops, convenience stores and bars, as well as on online platforms, including marketplaces or via classified advertisement sites dedicated to specific goods.

Case Study: Operation Thor

Due to persistently high levels of burglaries and thefts during the winter months, An Garda Síochána introduced an operation in 2015 as a strategic initiative to tackle these crimes. The operation is timed to coincide with the darker months of the year, running from 1 October to 31 March, when criminal activity typically increases due to reduced daylight. The operation combines high-visibility policing, targeted enforcement against OCGs and repeat offenders, and proactive crime prevention advice.

Since its launch, Operation Thor has had a significant impact. Residential burglaries during the winter months have decreased by 75%, demonstrating the effectiveness of the initiative. In 2024 alone, the operation led to over 2,000 arrests for burglary and related offenses. This success stands in contrast to international trends, where burglary rates tend to rise during winter, highlighting the strength of Ireland's targeted approach.

[48] Europol/ How COVID-19-related crime infected Europe during 2020 / Available from https://www.europol.europa.eu/cms/sites/default/files/documents/how_covid-19-related_crime_infected_europe_during_2020.pdf / p. 11
[49] Eurostat. (2025). Crime statistics - Statistics Explained. Available from https://ec.europa.eu/eurostat/statistics-explained/index.php?oldid=672448

Law Enforcement Intelligence

Intelligence indicates that certain OCGs are structured specifically to carry out targeted and, in some cases, armed robberies across Ireland. These incidents, though not as frequent, can yield substantial cash proceeds, with individual robberies generating up to €300,000. However, robbery of cash or goods in transit has been on a steady decline with 35 incidents in 2019 but just four recorded in 2024. Revenues generated from these robberies are typically laundered using cash-based techniques such as placing proceeds into cash-intensive businesses, purchasing high-value goods, and smuggling cash abroad. Although there are known OCGs which conduct theft and burglary, most theft and burglary incidents are not linked to OCGs. Where there are links to OCGs, stolen goods are typically moved quickly and often abroad to avoid detection and are targeted for resale through informal marketplaces, organised resale channels, HVGDs, and increasingly, online selling platforms. This resale activity facilitates the integration of criminal proceeds into the financial system, with some funds transferred internationally.

Illicit Trade and Smuggling

Rating

Smuggling and illicit trade generate proceeds through trafficking goods outside legal frameworks, with activity and seizure volumes rising steadily in recent years. While comprehensive economic impact data remains limited, law enforcement intelligence points to a well-organised and expanding illicit market, with laundering occurring through both domestic and international channels. This offence is assessed as posing a moderate ML threat.

Overview

Illicit Tobacco

Illicit tobacco products are those sold or supplied in Ireland without the payment of appropriate customs duties and taxes. They fall into two main categories, cigarettes and pouch tobacco. In respect of cigarettes, there are three classifications:

1. **Contrabands** account for 98% of the illicit tobacco trade, and are typically commercial brands purchased duty-paid or duty-free outside the country and then smuggled in. In 2023 and 2024, large quantities of illicit cigarettes of various brands were detected, believed to have originated in Bulgaria, where they were purchased by organised crime groups at lower prices before being smuggled into Ireland and onward to the UK.

2. **Counterfeits** are cigarettes illegally produced and then sold unlawfully either in the same jurisdiction or smuggled into another country where they are then sold unlawfully. Most counterfeit cigarettes seized in Ireland are believed to originate from Poland and Belgium, which have the highest detection rates of illicit production facilities in Europe. Two counterfeit manufacturing facilities have been detected and dismantled by Revenue in the last two years: one in Dublin 11 in February 2024 and the second in Ardee, Co. Louth in March 2025.

3. **"Illicit Whites"** are cigarettes manufactured legally but without the authorisation of the trademark owners, with intent for smuggling and sale in markets to avoid regulations and taxes. These typically originate from third countries such as the United Arab Emirates, Turkey, Singapore, Cambodia, and China, and are shipped via container traffic through major European ports before continuing to Ireland on feeder vessels.

Between 2020 and 2024, Revenue seized a total of 343.3 million illegal cigarettes and 106.9 tonnes of tobacco, with a value of over €307.2 million,[50] and associated estimated losses to Revenue in the same period of over €1.8 billion.[51]

Table 14: Number of seizures and estimated value from illicit tobacco (2020 – 2024)

Seizures	2020	2021	2022	2023	2024
Number of Seizures and Detections	4,436	6,581	6,884	6,837	6,420
Total Value of Illegal Tobacco and Cigarettes Seized by Revenue (€m)	37.0	67.6	48.0	63.4	128.2

In 2024, the value of tobacco seizures by Revenue more than doubled compared to 2023, with major seizures highlighting the scale of Ireland's illicit tobacco trade, driven wholly by high excise duties, making illegal products attractive within the shadow economy.

Recent Significant Seizures by Revenue Include:

- 14.6 million cigarettes seized in Dublin in February 2024, with an estimated retail value of €12 million, representing a potential loss to the Exchequer of approximately €9.6 million.
- 13.3 million cigarettes seized in Dublin Port in March 2024, with an estimated retail value of €11 million, representing a potential loss to the Exchequer of approximately €8.9 million.
- €5 million worth of tobacco seized in Dublin Port in March 2024, representing a potential loss to the Exchequer of over €3.7 million.
- Over 20 million cigarettes seized in separate operations in Rosslare Europort in July and August 2024, with an estimated combined retail value of over €16.3 million, representing a potential loss to the Exchequer of approximately €12.8 million.
- 1,200 kg of chewing tobacco worth €660,000 seized at Dublin Port, arriving via the Netherlands in November 2024.

[50] Revenue Annual Report 2020 – 2024, Excisable Products Seized / Available from: https://www.revenue.ie/en/corporate/press-office/annual-report/index.aspx?year=2020
[51] Annual Illegal Tobacco Products Research Surveys conducted by Ipsos MRBI on behalf of Revenue and HSEs National Tobacco Control Office / Available from: https://www.revenue.ie/en/corporate/information-about-revenue/statistics/surveys/tobacco-consumption/index.aspx

Arms Trafficking

Firearms trafficking within the EU remains limited in scale, with most weapons smuggled to fulfil specific orders or for personal use. This illicit trade often intersects with drug trafficking, with firearms smuggled from Eastern Europe to support drug-related operations. Illicit firearms trafficking is a national priority and the seizure referred to below from July 2024 in Louth is an example of how a recently identified firearms trafficking route into Ireland was dismantled.

Case Study: Seizure of Multiple Weapons from OCGs

In April 2024, An Garda Síochána conducted over 20 intelligence-led, coordinated search operations across various units in Dublin, targeting OCGs. These operations resulted in the seizure of multiple firearms and associated items, including:

- One semi-automatic machine pistol and nine rounds of ammunition.
- Two firearms recovered during a targeted search of a public park.
- Seven firearms with associated ammunition, alongside significant quantities of cannabis and cocaine, with an estimated combined street value of €200,000. Approximately €100,000 in cash was also recovered, underscoring the strong link between drug trafficking and the possession of illegal firearms, as well as the continuing use of cash as criminal proceeds.

Additionally, in July 2024, An Garda Síochána seized 18 firearms and approximately 900 rounds of ammunition at a premises in Co. Louth. During this search, Gardaí seized six assault rifles and twelve semi-automatic handguns.

Counterfeit Currency

In 2024, approximately 554,000 counterfeit euro banknotes were removed from circulation in the euro area, with 18 counterfeit notes detected per million genuine banknotes; this is comparatively low by historical standards. Counterfeiting of the €20 and €50 denomination notes continue to be the most common, together accounting for over 75% of all detected counterfeits. Of the total counterfeits identified, 97.8% were found within euro area countries, 1.3% in non-euro area EU Member States, and 0.9% in other regions worldwide.[52] Trends in Ireland broadly track those in the euro area. As shown in Table 15 below, there has been a

[52] European Central Bank / Press Release: Number of counterfeit euro banknotes continues to be low in 2024 / Available from: https://www.ecb.europa.eu/press/pr/date/2025/html/ecb.pr250221~c0d1113d2c.en.html

recent increase in reported counterfeit currency incidents reported to An Garda Síochána. More counterfeit incidents – often single piece detections – are reported to the Central Bank.

Table 15: Reported counterfeit currency incidents (2021 – 2024)

Counterfeit Currency	2021	2022	2023	2024
No. of Incidents	285	218	176	746

Most counterfeits across the euro area originate from Italian OCGs,[53] with other significant sources including China, Taiwan, and Turkey. The rise of the darknet and e-commerce platforms hosted in Asia has transformed distribution channels, including for raw materials for counterfeit notes, often linking counterfeiters to broader networks of drug and contraband traders. The Central Bank notes that indigenous counterfeit operations exist across the euro area, including Ireland, although the last counterfeit banknote production facilities at scale in Ireland were shut down in the mid-2010s.

Environmental Crimes

Environmental crimes, including illegal wildlife trade, illegal logging and illegal waste management, are inherently transnational crimes that converge with other crimes such as corruption and pose a systemic threat to biodiversity. FATF considers environmental crime to be amongst the most profitable illicit activities, estimating annual proceeds between $110b and $281 billion.[54]

While environmental crime is a growing global concern, the threat landscape in Ireland is comparatively less significant, in part due to its limited domestic natural resources, effective environmental protection laws and comparatively low levels of corruption. However, the FATF notes that even countries with limited natural resources are vulnerable due to the transnational nature of environmental crimes and their links to other illicit activities. In the Irish context, the Environmental Protection Agency ("EPA") has identified metal theft and the misclassification of waste as two notable and ongoing environmental threats.

Metal theft continues to be a persistent issue, driven in part by the global increase in metal prices. First highlighted in the 2014–2020 National Hazardous Waste Management Plan,[55]

[53] Europol / EU Serious and Organised Crime Threat Assessment (EU SOCTA) 2025 / p. 73
[54] FATF/ FATF Report Money Laundering from Environmental Crime July 2021 / Available from: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Money-Laundering-from-Environmental-Crime.pdf / p.7
[55] Environmental Protection Agency, National Hazardous Waste Management Plan, 2014-2020 / Available from: https://www.epa.ie/publications/monitoring--assessment/waste/hazardous-waste/national-hazardous-waste-management-plan-2014---2020.php/ p. 40

this issue remains a challenge at EPA-licensed facilities.[56] Misclassification of waste (i.e. the deliberate act of incorrectly identifying waste types to evade higher disposal fees and taxes) also remains a concern. Dublin City Council is designated as the competent authority in Ireland for the export and import of waste shipments and transit of hazardous waste within Ireland.

Fuel Smuggling

In 2024, Revenue seized 156,960 litres of illicit fuel[57] (estimated value of €267,000), representing an increase of 57% compared to the 99,895 litres seized in 2019.[58] This rise is attributed to improved enforcement capabilities, particularly following the introduction of the EU fuel marker Accutrace Plus in January 2024.

Fuel laundering operations have been identified on both sides of the border in Ireland, with OCGs from both Ireland and Northern Ireland involved. Although the specific payment methods remain unknown, patterns suggest covert activity and misrepresentation of product origin. Illicit fuel is likely sold in bulk to high-volume users and may be diverted into legitimate wholesale and retail channels.

Case Study A: Illicit Fuel Seizure

In May 2025, as part of an intelligence-led operation, Revenue's Customs Service, supported by the State Laboratory, detected suspected laundered fuel for sale at two filling stations and at a fuel distributor premises in Co. Louth. The premises were searched under warrant, and 55,000 litres of fuel were removed for further examination.

Case Study B: Illicit Mineral Oil Seizure

In April 2024 Revenue officers seized 40,500 litres of marked mineral oil with an estimated retail value of over €66,200 in Co. Tipperary. The illicit fuel was discovered during the search of a haulage yard and represented a potential loss to the Exchequer of approximately €34,800.

[56] Information provided by the Environmental Protection Agency
[57] Revenue / Annual Report 2024 / Available from: https://www.revenue.ie/en/corporate/press-office/annual-report/2024/ar-2024.pdf / p. 58
[58] Revenue / Annual Report 2019 / Available from: https://www.revenue.ie/en/corporate/press-office/annual-report/2019/ar-2019.pdf / p. 12

Illicit Alcohol Smuggling

Smuggled alcohol consignments have been detected entering the State from various EU Member States. In 2024, Revenue seized over 595,000 litres of illicit alcohol, valued at an estimated €3.2 million.[59] This represents an increase of 9.5% in volume compared to 543,194 litres seized in 2019, although the value of the seized alcohol declined from €3.3 million in 2019.[60]

OCGs from both Ireland and Northern Ireland have been identified as being involved in these operations. Revenue is aware of instances where false paperwork has been used to accompany mis-manifested alcohol shipments. It is believed that most significant alcohol smuggling activity in Ireland involves transit routes between mainland Europe and the UK. While some illicit alcohol may enter the Irish market, the majority is believed to be moved onward to the UK for sale.

Case Study: Illicit Alcohol Seizure

In November 2024, as a result of risk profiling, Revenue officers seized 207,369 litres of alcohol, with an estimated value of €1,094,751, at Dublin Port. The illicit alcohol consisted of approximately 174,744 litres of beer, which represented a potential loss to the Exchequer of over €326,000. It also consisted of approximately 32,625 litres of wine, which represented a potential loss to the Exchequer of over €212,000. The consignment was seized when Revenue officers stopped and searched 9 containers that arrived from Rotterdam.

Illicit Trafficking in Cultural Goods; Antiquities, Artworks

Trafficking in cultural property is a low-risk, high-profit business for criminals linked to organised crime, and the market's characteristics, such as high-value transactions and lack of transparency, make it vulnerable to misuse.[61] However, there is limited evidence to suggest that illicit trafficking in cultural goods poses a significant threat within Ireland.

[59] Revenue / Annual Report 2024 / Available from: https://www.revenue.ie/en/corporate/press-office/annual-report/2024/ar-2024.pdf / p. 47
[60] Revenue / Annual Report 2019 / Available from: https://www.revenue.ie/en/corporate/press-office/annual-report/2019/ar-2019.pdf / p. 33
[61] FATF/ Money Laundering and Terrorist Financing in the Art and Antiquities Market 2023/ Available from: https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/Money-Laundering-Terrorist-Financing-Art-Antiquities-Market.html / p. 16

Illicit Trafficking in Hormonal Substances

The Health Products Regulatory Authority ("HPRA") in Ireland classifies illicit hormonal substances, such as anabolic steroids and other performance-enhancing drugs, as prescription-only medicines that are imported, sold, or distributed without authorisation. These substances are often sourced online or smuggled into the country, bypassing regulatory controls and posing health risks. They typically fall into three categories:

- Unauthorised Imports: Legitimate prescription products purchased abroad and brought into Ireland illegally for distribution.
- Counterfeits: Fake products that imitate genuine medicines but may contain harmful or incorrect ingredients.
- Mislabelled or Falsified Products: Substances deliberately misrepresented in terms of content, origin, or use.

In 2024, the HPRA detained over 1 million units of illegal medicines, representing a 14% increase from 2023, with anabolic steroids accounting for 203,088 units. This marked a 20% rise in illicit anabolic steroid seizures compared to the previous year. The data highlights that anabolic steroids, sedatives and erectile dysfunction products are consistently the most detained categories of illegal medicines year-on-year.[62]

The HPRA also noted an upward trend in detentions of GLP-1 (diabetes and weight loss medicines) products including, predominantly, semaglutide and liraglutide. While overall numbers remain low, there was a significant upturn in seizures, with 1,582 units of GLP-1 products seized in 2024 compared to 568 units in 2023 and just 40 units in 2022.

Table 16: Yearly illegal medicines detention figures by HPRA from (2020 – 2024)

2020	2021	2022	2023	2024
1.6m (+61%)	1.6m (-1%)	0.9m (-40%)	0.9m (-8%)	1m (+14%)

As part of its enforcement remit, the HPRA conducts ongoing monitoring to identify illegal online activity promoting prescription medicines and other substances to consumers. It routinely intervenes to disrupt online promotions through website closure and social media page removals. The HPRA also initiates prosecution cases where it considers that there is a significant risk to public health or where there are persistent non-compliances. In 2024, the

[62]HPRA / Over 1 million units of illegal medicines detained by the HPRA in 2024 / https://www.hpra.ie/news-events/news/article/over-1-million-units-of-illegal-medicines-detained-by-the-hpra-in-2024#:~:text=Over%20one%20million%20units%20of,other%20illegal%20medicines%20in%202024.

HPRA undertook several significant enforcement actions in close collaboration with An Garda Síochána and Revenue. This inter-agency cooperation continues to be a key element in combating the illegal supply of health products into and within Ireland, including:

- Two prosecution cases initiated, one relating to the importation or distribution of anabolic steroids and one relating to the importation or distribution of the weight loss product Saxenda;

- 2,553 websites, e-commerce listings and/or social media pages amended or shut down.

Law Enforcement Intelligence

Due to high excise duties – particularly on tobacco, alcohol, and fuel – illicit trade and smuggling activities provide lucrative profit margins for criminal networks. These operations are often cash-intensive, relying on traditional payment methods to obscure financial trails. However, certain segments, especially those involving cross-border trafficking and high-value goods, increasingly leverage digital payment systems and virtual assets. Intelligence assessments indicate a well-organised and expanding illicit market, posing a ML threat through both domestic and international channels.

Human Trafficking and Exploitation

Rating

Human trafficking is the second most widespread illicit economic activity globally,[63] with both international and domestic OCGs exploiting the movement of migrants and other vulnerable groups. As a developed country, Ireland is highly susceptible to such offences. The level of proceeds generated by human trafficking in Ireland is difficult to quantify. Perhaps owing to its geographic circumstances, available quantitative data indicate that, in a domestic context, the problem of human trafficking in Ireland is less severe than that which affects other jurisdictions. As a result, human trafficking is considered to be a moderate ML threat.

Overview

Human trafficking[64] remains a substantial criminal market within the EU, particularly for sexual and labour exploitation,[65] and generates an estimated $236 billion annually.[66] The Chief Commissioner of the Irish Human Rights and Equality Commission has noted that it is the fastest growing criminal industry in the world.[67]

The human trafficking threat is increased by geopolitical instability and conflict, leading to an increase in the number of displaced people, who are vulnerable to targeting by criminal gangs. At the end of 2024, over 120 million individuals were forcibly displaced globally (an increase of 6% on 2023 and an increase of almost 50% during the previous decade),[68] all of whom are at increased risk of becoming trafficking victims.

The laundering of proceeds from human trafficking varies depending on the form of exploitation and the method by which illicit funds are generated. In cases involving sexual exploitation and forced labour the activity is typically cash-based, though increasingly shifting to digital banking and financial platforms, and often involving international elements. Criminal

[63] European Commission / combating trafficking in human beings (Fifth Report) / eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025DC0008 / p. 1
[64] Defined in Article 2 of EU Directive 2011/36/EU, as the recruitment, transportation, transfer, harbouring or reception of persons by means of threat, force, coercion, abduction, fraud, deception or abuse of power for the purpose of exploitation. Amended by Directive (EU) 2024/1712 to expand exploitation to include sexual exploitation, forced labour, slavery, servitude, exploitation of criminal activities, removal of organs, and new forms such as forced marriage, illegal adoption and surrogacy. The amended Directive must be transposed into Irish law by 15 July 2026.
[65] Europol, The changing DNA of serious and organised crime 2025 / Available from: https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime / p. 47
[66] European Commission/ Report from The Commission to the European Parliament, The Council, The European Economic and Social Committee and The Committee of the Regions on the progress made in the European Union in combating trafficking in human beings (Fifth Report) 2025/ Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025DC0008 / p. 1
[67] Irish Human Rights and Equality Commission / Commission calls for equal treatment and an end to punishment of victims / https://www.ihrec.ie/news-press/state-makes-progress-but-crucial-gaps-remain-in-protection-of-victims-of-human-trafficking
[68] United Nations High Commissioner for Refugees (2024) Global Trends: Forced Displacement in 2024 / p.6

networks engaged in these operations are known to use financial institutions, money remittance providers, and VASPs, as well as using IVTS and cash smuggling to move funds across borders and evade detection.

European Context

Between 2021 and 2022, the number of registered trafficking victims in the EU increased by more than 20%, with most victims being non-EU citizens (54%), and 49% of victims being used for the purpose of sexual exploitation.[69] In 2023, the upward trend continued, with 10,793 victims registered, a 6.9% increase from the previous year. The proportion of women and girls rose to more than 63%, and sexual exploitation remained the predominant form at over 43%.[70] The top five non-EU nationalities of victims identified in 2021-2022 were Nigerian, Ukrainian, Moroccan, Colombian, and Chinese.[71] Europe is one of the most profitable locations for the exploitation of human trafficking victims, with profits estimated at $20,000 per victim per year; this figure has increased by 37% since 2014.[72]

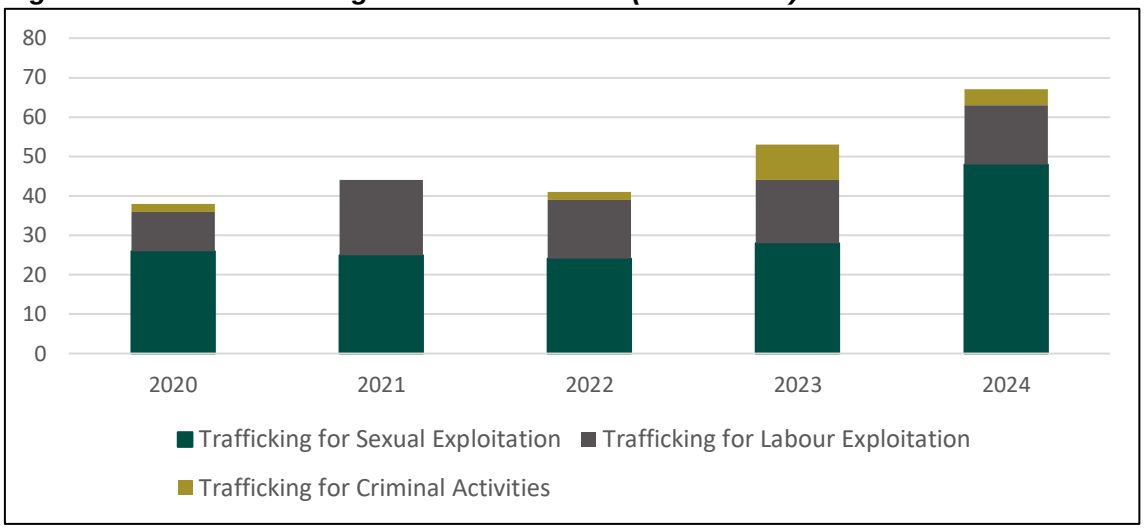
Human Trafficking in Ireland

Ireland is increasingly recognised as a destination country for human trafficking. While not a major source of trafficked individuals, its economic opportunities make it attractive to traffickers targeting vulnerable populations from specific regions, including West Africa (particularly Nigeria), Eastern Europe (particularly Romania), Southeast Asia, and South America (particularly Brazil). Victims are often trafficked into Ireland under false promises of employment, education, or safety, only to face exploitative conditions upon arrival. Ireland is also increasingly being used as a transit route to the UK, a shift driven largely by Ireland's unique situation of being an EU member state and having a Common Travel Area between Ireland and the UK.[73]

[69] European Commission (2025) Commission Staff Working Document / Statistics and trends in trafficking in human beings in the European Union in 2021–2022. SWD (2025) 4 final / Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025SC0004 / p. 2
[70] Eurostat, 2025. Trafficking in human beings statistics. [online] European Commission. Available from: https://ec.europa.eu/eurostat/statistics-explained/index.php?oldid=684698
[71] European Commission (2025) Commission Staff Working Document / Statistics and trends in trafficking in human beings in the European Union in 2021–2022. SWD (2025) 4 final Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025SC0004 / p. 8
[72] European Commission// Report from The Commission to the European Parliament, The Council, The European Economic and Social Committee and The Committee of the Regions on the progress made in the European Union in combating trafficking in human beings (Fifth Report) 2025/ Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025DC0008 / p.1
[73] Global Initiative Against Transnational Organised Crime / Organised Crime Index – Ireland / Available from: https://ocindex.net/assets/downloads/2023/english/ocindex_profile_ireland_2023.pdf / p. 5

Although the total case numbers in Ireland remained at stable levels between 2020 and 2022, there was an increase in identified victims between 2022 and 2023 of 20%.[74] This is partly a result of increased capacity to detect human trafficking in Ireland but may also be indicative of an increase in human trafficking activity. Ireland's National Rapporteur for human trafficking has noted that 40% or more of human trafficking cases are never identified due to the characteristics of human trafficking, including its clandestine nature and its overlap with other illegal activities.[75]

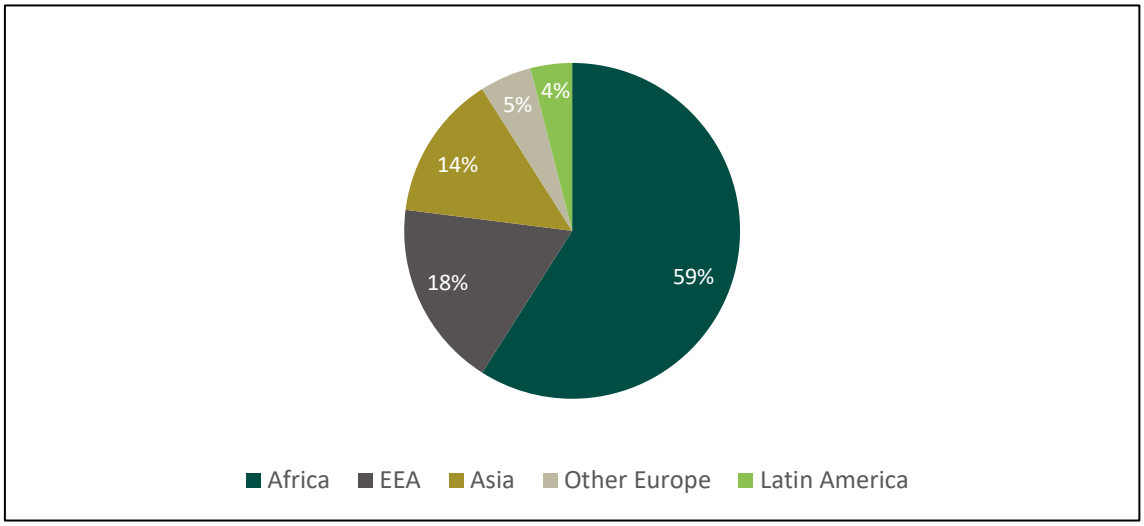
Figure 4: Human trafficking victims and trends (2020 - 2024)[76,77]



Human trafficking in Ireland continues to be a highly gendered and racialised crime, with 68%[78] of victims being women, and nearly all victims being of migrant background. Children account for 8% of all identified victims of trafficking in Ireland (44 children in total from 2013 to 2023), which is lower than the EU average of 15%. In 2022 and 2023, ten suspected child victims of trafficking were identified, eight girls and two boys. The majority were victims of Trafficking for Sexual Exploitation ("TSE") (6), followed by Trafficking for Criminal Activities ("TCA") (3), and Trafficking for Labour Exploitation ("TLE").

[74] IHREC / Trafficking in Human Beings in Ireland 2023: Third Evaluation of the Implementation of the EU Anti-Trafficking Directive / Available from: https://www.ihrec.ie/downloads/Trafficking-in-Human-Beings-in-Ireland-2023-4.pdf / p. 404
[75] Ibid., p. 404
[76] Ibid., p. 400
[77] IHREC (2025) / Ireland's Actions Against Trafficking in Human Beings: Submission to the Council of Europe Group of Experts on Action against Trafficking in Human Beings (GRETA) on the implementation of the Council of Europe Convention on Action against Trafficking in Human Beings Fourth Evaluation Round Irish Human Rights and Equality Commission / Available from: https://www.ihrec.ie/uploads/banners/HTML/uploads/banners/26082025-IHREC-NR-Report-to-GRETA_Final.pdf / p.8
[78] Trafficking in Human Beings in Ireland 2023: Third Evaluation of the Implementation of the EU Anti-Trafficking Directive / p. 7

Figure 5: Victims of trafficking by region of origin (2022 – 2024)[79]



Trafficking for Sexual Exploitation: TSE remains the most prevalent form of human trafficking in Ireland, accounting for 55% of reported cases between 2013 and 2023. It is also the most gendered, with 96% of victims being female. While this form of trafficking was predominantly a cash-based illicit activity, it is increasingly shifting transactions to digital platforms.

Trafficking for Labour Exploitation: 38% of reported human trafficking cases between 2013-2023 in Ireland related to TLE. This involves the coercion of individuals into forced labour under exploitative conditions, often involving threats, debt bondage, or withholding of wages. Victims of TLE in Ireland are predominantly (68%) male; of the 21 cases reported in 2023, two-thirds (14) of the victims were forced to work in restaurants, domestic work or bakeries.

Trafficking for Criminal Activities: Approximately 7% of reported human trafficking cases between 2013-2023 in Ireland related to TCA. TCA victims are exploited to conduct a variety of criminal activities, including fraud, money muling, drug dealing or production (e.g., operation of cannabis grow houses). These victims are often vulnerable, for example due to immigration status, addiction, or due to disability or illness.

<u>Online Sexual Exploitation of Children</u>

Online Sexual Exploitation of Children ("OSEC") is an increasingly concerning element within Ireland's broader human trafficking and exploitation landscape. While much of the

[79] IHREC (2025) / Ireland's Actions Against Trafficking in Human Beings: Submission to the Council of Europe Group of Experts on Action against Trafficking in Human Beings (GRETA) on the implementation of the Council of Europe Convention on Action against Trafficking in Human Beings Fourth Evaluation Round Irish Human Rights and Equality Commission / p.9

exploitative content is produced abroad, particularly in Southeast Asia – notably the Philippines – Ireland is impacted as a destination country for this material. International networks, including those identified in the Philippines, distribute content via encrypted platforms and the dark web, frustrating detection and disruption efforts.

The growth in OSEC is in part driven by widespread access to the internet and social media, including by children. As noted by the FATF, there is no reliable estimate of the proceeds generated globally by OSEC and Financial Sexual Extortion of Children ("FSEC"). However, both crime types are large in scale and becoming increasingly prevalent. While the financial gains are not considered significant in comparison to other predicate offences, concluded cases and victim reporting offer some insight into how proceeds are generated and laundered.

- OSEC payments typically range from €75–€200 and are made to facilitators in high-risk, developing countries. Transactions are usually processed through Peer-to-Peer ("P2P") platforms, bank transfers, or transfers of virtual assets through CASPs, which offer a degree of anonymity. OCG involvement is rare, though informal networks are active.[80]

- In FSEC involving ransom, payments are usually low, between €50 and €1,500, with initial demands often under €250, reflecting the limited means of teenage victims. Offenders may attempt to extract multiple payments by exploiting victims' shame, but these efforts are typically short-lived. When victims can no longer pay, they may be coerced into criminal activities such as money muling, extending the exploitation and drawing them into broader criminal activity.[81]

Case Study: Human Trafficking for TSE

Ireland secured its first conviction under the Criminal Law (Human Trafficking) Act in 2021, prosecuting two Nigerian women for trafficking victims from Nigeria via Libya and Italy to run a prostitution ring in Mullingar. Following appeals and further investigation, sentences were increased in 2023, and another member of the network was jailed in 2025.

Victims were found to have regularly deposited cash amounts ranging from €200 to €1,000 into Irish bank accounts over periods of six months to two years, generating an estimated €95,000 in criminal proceeds. An Garda Síochána traced some of these funds to Nigeria.

[80] FATF / Detecting, Disrupting and Investigating Online Child Sexual Exploitation / Available from: https://www.fatf-gafi.org/en/publications/Fatfgeneral/Online-child-sexual-exploitation.html / page 12
[81] Ibid. / page 15

Law Enforcement Intelligence

Human trafficking networks often exploit legitimate bank accounts, frequently opened by foreign nationals who later leave the jurisdiction, and use them to process the low-value, high-volume transactions generated by this activity. Payments for OSEC in Ireland are typically made in round currency amounts and paid via digital platforms and virtual assets. While Suspicious Transaction Reports ("STRs") are often filed relating to this activity, they can lack specificity about the nature of the underlying suspicion, though credit and financial institutions are cooperative with the provision of information. Cash also remains a key transfer mechanism for all forms of human trafficking and exploitation, particularly among Eastern European OCGs, who transit cash in bulk to Eastern European countries; there have been notable cash seizures relating to this activity in recent years.

Tax Crime

Rating

Tax offences generate illicit proceeds primarily through undeclared income and fraudulent activity which span multiple sectors including, but not limited to, the cash economy, trades, professional industries and legitimate businesses. These offences involve both opportunistic individuals operating in the shadow economy, as well as more sophisticated cases involving the use of complex financial structures. The threat is further compounded by the increasing complexity of digital and cross-border transactions, which hinder detection. As a result, tax offences are assessed as posing a moderate ML threat.

Overview

Tax crime in Ireland refers to deliberate acts or omissions intended to evade tax obligations, as defined under Section 1078 of the Taxes Consolidation Act 1997. These offences include knowingly submitting false tax returns or documentation, unlawfully claiming tax reliefs or refunds, and failing to remit specific taxes. Tax offences in the context of smuggling, such as evasion of excise duties and customs charges, are addressed in the illicit trade and smuggling threat assessment. These crimes typically involve the illicit importation of goods, and while they constitute tax offences, they are assessed separately to ensure a focused analysis of smuggling-related activities.

The Irish shadow economy[82] involves businesses and individuals engaging in practices that evade obligations such as taxes, PRSI, licences, customs duties and employment regulations. Common activities include underreporting income, paying employees “off the books”, falsely claiming welfare benefits while working, evading VAT, and illegal trades like tobacco smuggling and fuel laundering.[83] Cash-based industries, notably construction, hospitality, fast-food outlets, entertainment, and retail, present elevated risks of tax evasion because limited traceability increases opportunities for under-reporting.[84] The opacity, informality, routine use of cash, absence of proper bookkeeping, and limited oversight within the shadow economy create a conducive environment for ML, especially through layering

[82] The shadow economy refers to income-generating activities that are not reported to authorities and are designed to avoid taxation, regulation, or government oversight. This includes unregistered businesses, ‘cash-in-hand’ jobs, illegal trade like smuggling or counterfeit goods, and underreporting income or sales.
[83] Revenue / Reporting tax evasion (shadow economy activity) Available from: https://www.revenue.ie/en/corporate/assist-us/reporting-shadow-economy-activity/index.aspx
[84] European Labour Authority / Factsheet on undeclared work – Ireland / Available from: https://www.ela.europa.eu/sites/default/files/2024-02/IE-UDW_factsheet-2023-fin.pdf?utm / p.4

and the integration of the illicit proceeds, hindering the detection of both tax evasion and associated laundering activities.

Ireland does not conduct a holistic tax gap analysis – although assessments of potential tax losses associated with specific activities or sectors of the economy where compliance issues are identified are undertaken – which makes estimating the total value of criminal proceeds from tax offences in Ireland difficult. Illicit funds from tax evasion are often integrated through routine spending, making detection challenging. More complex cases often involve the misuse of companies and trusts to conceal income and beneficial ownership, aided by professional enablers who structure opaque financial arrangements. In some cases, cash-based laundering is also used, particularly in cash-intensive businesses, to disguise undeclared income and integrate it into the financial system.

International reviews continue to recognise Ireland as maintaining an efficient, transparent tax system, which is well aligned with international standards. For example, the 2023 OECD peer review under the Forum on Harmful Tax Practices highlighted Ireland's strong commitment to transparency and cooperation in exchanging tax rulings.[85] Ireland's commitment to maintaining a transparent and cooperative tax environment is further reinforced through its participation in a broad range of international tax treaties and frameworks. These include double taxation agreements, tax information exchange agreements, and the OECD's Multilateral Convention to Implement Tax Treaty Related Measures to prevent Base Erosion and Profit Shifting.

The increasing use of virtual assets such as cryptocurrencies presents significant challenges to tax compliance and enforcement. Bodies including the OECD and the European Commission have acknowledged that the decentralised and pseudonymous nature of these assets complicates detection of undeclared income and capital gains. To address these risks, the OECD's Crypto-Asset Reporting Framework and the EU's Directive on Administrative Cooperation (8th iteration) mandate enhanced reporting and information sharing by crypto service providers.

[85] Harmful Tax Practices – 2023 Peer Review Reports on the Exchange of Information on Tax Rulings / Available from: https://www.oecd.org/en/publications/harmful-tax-practices-2023-peer-review-reports-on-the-exchange-of-information-on-tax-rulings_efbad00d-en/full-report/ireland_628c5e23.html?utm / p. 201-

Law Enforcement Intelligence

In 2024, Revenue secured 148 summary convictions for tax-related offences, with court fines totalling €385,520. Additionally, 20 indictable convictions for tax and duty evasion were secured before the courts, comprising:

- 9 convictions for tax offences.
- 11 indictable convictions for duty offences.

In 2024, Revenue referred 14 suspected tax and excise evasion cases to the ODPP, who directed indictable proceedings in all 14. By year-end, 20 cases of tax evasion or fraud remained under investigation, with a further 34 pending before the courts.

A total of 168 prosecutions for tax and duty offences were secured in 2024, resulting in total fines of €401,520.[86]

Table 17: Revenue action on tax (2020 – 2024)[87]

Revenue Report Findings	2020	2021	2022	2023	2024
Prosecutions for tax and duty offences[88]	248	231	162	190	168
Fines relating to tax and duty offences	€895,545	€599,699	€416,840	€554,180	€401,520
Criminal convictions	21	6	9	21	20

[86] Revenue Commissioners (2025)/ Annual Report 2024/ Dublin: Office of the Revenue Commissioners/ Available from: https://www.revenue.ie/en/corporate/press-office/annual-report/2024/ar-2024.pdf / p.17
[87] Revenue Commissioners, Annual Reports, 2019-2024.
[88] Indictable tax and duty evasion is considered to arise where the tax default cannot be attributable to insufficient care/carelessness but rather there are indications of deliberate behaviour through an examination of records or from discussions with the taxpayer.

Cybercrime

Rating

Cybercrime is generating substantial proceeds and is globally recognised as a highly organised criminal activity, often led by OCGs and state actors. Ransomware attacks, in particular, can yield profits ranging from tens of thousands to hundreds of millions of euro. Criminals exploit digital platforms and crypto-assets to launder funds rapidly and anonymously. The threat is amplified by under-reporting, cross-border enforcement challenges, and the emergence of tools such as Ransomware-as-a-Service ("RaaS"). Despite limited domestic financial indicators, the global nature and laundering potential of cybercrime justify its classification. While cybercrime is deemed to be of considerable importance with regard to ML and PF globally, there is limited evidence of proceeds being generated or laundered domestically. Cybercrime is therefore assessed as posing a low ML threat. Cyber-enabled fraud is assessed separately in the fraud section.

Overview

Cybercrime is using information technology to perpetrate or facilitate a crime. Examples include unauthorised access of data, interference with computer systems or data, deliberate injection of viruses or encryption malware (ransomware) into a system or denial of service attacks. Europol estimates that cybercrime is likely to be under-reported and that it represents an increasing threat for individuals, businesses, and governments.[89] The criminal cyber threat landscape remains wide-ranging, comprising both lone actors and networks with various levels of expertise and capability. Some cybercriminals targeting the EU are EU-based, while others operate from third countries and can be connected to nation states.[90]

Cybercrime in Ireland is primarily conducted through ransomware attacks, which have shifted from targeting large enterprises to small and medium-sized businesses. The rise of RaaS has made it easier for less sophisticated actors to launch impactful attacks, often without deep system access. While domestic reporting remains stable, the true scale is extremely difficult to quantify due to the borderless nature of these crimes, and the use of virtual payment channels and cryptocurrencies to launder proceeds. Cybercrime actors operate with the use of complex and well organised ML networks, exploiting 'cold wallets' (a cryptocurrency wallet which is disconnected from the internet), privacy coins, and cross-chain

[89] Europol / Internet Organised Crime Threat Assessment (IOCTA) / 2023 / Available from: https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202023%20-%20EN.pdf?utm_source=copilot.com
[90] Europol / Internet Organised Crime Threat Assessment (IOCTA) / 2024 / Available from: https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf

transactions to obscure funds, making detection and prosecution challenging, especially when actors operate from non-cooperative jurisdictions. However, Ireland's growing engagement with international partners continues to improve intelligence sharing, asset tracing, and disruption efforts.

Threat from State Backed Actors

Nation-state actors are a significant threat in the cybercrime landscape, with geopolitical instability, particularly linked to Russia, China, and North Korea, driving increased activity.[91] These actors exploit zero-day vulnerabilities,[92] target critical infrastructure and supply chains, and may also be engaged in espionage against EU institutions and industries. Their operations may be politically or financially motivated, as seen with groups like North Korea's Lazarus Group, which engages in large-scale cybercrime to bypass sanctions and fund state proliferation programmes.[93]

Threat from Cybercriminals

Ireland is facing a growing threat of increasingly sophisticated cybercriminal groups, particularly ransomware operators, which have grown in sophistication and impact. The rise of RaaS has lowered barriers to entry to committing cybercrime, and in 2020 two-thirds of ransomware campaigns were attributed to operators using RaaS. Attackers increasingly exploit remote work infrastructure, use social engineering, and multi-extortion tactics involving data theft and public exposure to coerce victims into paying ransoms. Cybercrime-as-a-Service ecosystems have also emerged, offering phishing kits, malware, and laundering tools which has further expanded the threat landscape.

Hacktivists and Terrorist-Aligned Actors

Hacktivists and terrorist-aligned actors often aligned with geopolitical conflicts or ideological causes are also a key threat group. Groups supporting geopolitical conflicts have demonstrated increased capability, conducting Distributed Denial of Service ("DDoS") campaigns and ransomware attacks. These actors' capabilities are advancing, and their growing sophistication raises concerns about unintended spillover, which may facilitate the recruitment of such individuals into more serious criminal or state-sponsored activity.

[91] Department of Justice, Home Affairs and Migration. National Cyber Risk Assessment 2022. Available from: https://www.gov.ie/en/department-of-justice-home-affairs-and-migration/publications/national-cyber-risk-assessment-2022/ pg. 5
[92] A vulnerability which is not known to the software or hardware developer
[93] Department of Justice, Home Affairs and Migration. National Cyber Risk Assessment 2022. Available from: https://www.gov.ie/en/department-of-justice-home-affairs-and-migration/publications/national-cyber-risk-assessment-2022/ p. 7

'Script kiddies' – less technically skilled individuals who use pre-built tools – can amplify these threats by participating in or enabling such campaigns, often without fully understanding the broader implications of their actions. Their involvement can serve as a gateway into more organised or ideologically driven cybercrime.

The Evolving Cyber Threat: Insights from Ireland and Worldwide

In Ireland, ransomware attacks have increasingly targeted organisations across critical sectors, including manufacturing, energy, IT, healthcare, transportation, and education. In 2024 alone, more than 49 confirmed ransomware incidents were reported, highlighting the growing sophistication and persistence of cybercriminals operating within the region. Despite these developments, Ireland recorded the lowest rate of organisations experiencing a cyber-attack in the past 12 months, with 42% reporting at least one incident. This contrasts sharply with Germany and the United Kingdom, where 67% and 65% of organisations respectively faced similar threats. These figures suggest that while Ireland remains comparatively less exposed, it is still vulnerable to targeted attacks on essential industries.

Globally, the threat landscape has evolved at an unprecedented pace. China-nexus activity surged by 150% across all sectors, with certain industries experiencing increases of between 200% and 300%. Social engineering-based attacks also intensified, with vishing incidents skyrocketing by 442% between the first and second halves of 2024. These trends reflect a shift toward highly agile and stealthy attack methodologies, where adversaries exploit human vulnerabilities and systemic weaknesses to gain rapid access and escalate privileges. The combination of ransomware proliferation in Ireland and accelerating global attack dynamics illustrates the critical importance of proactive defence strategies, robust identity controls, and comprehensive incident response capabilities.[94]

[94] CrowdStrike / 2025 Global Threat Report / Available from: https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrikeGlobalThreatReport2025.pdf?version=0 / p.10

Case Study: Health Service Executive ("HSE") Cyber-attack

The HSE is Ireland's public health and social care service. On 14 May 2021, the HSE was subjected to a cyber-attack, through the criminal infiltration of its IT systems using 'Conti' ransomware, which caused all of its IT systems nationwide to shut down. It was the most significant cyber-attack on an Irish State agency, as well as the largest known attack against a health service computer system in history, and occurred during the COVID-19 pandemic.

The malware infection was the result of the user of the Patient Zero Workstation clicking and opening a malicious Microsoft Excel file that was attached to a phishing email. An investigation into the breach found that the HSE was operating on a frail IT system and did not have proper cyber expertise or resources.

Law Enforcement Intelligence

Cybercriminals are exploiting system vulnerabilities, outdated credentials, and zero-day vulnerabilities to gain access to networks, with ransomware remaining the dominant method of attack. Once inside, they move quickly to monetise their access, primarily through virtual assets like cryptocurrencies. Laundering is carried out using cold wallets, the use of privacy coins, and cross-chain bridges, which obscure the flow of funds and make tracing difficult until the point of converting to fiat currencies; this 'cash-out' stage is often the only viable opportunity for law enforcement to identify suspects. Prosecution is difficult due to the borderless nature of cybercrime. Many actors also operate from jurisdictions that do not cooperate with international investigations, which creates barriers to attribution and legal action. Despite these challenges, Ireland is seeing progress through deeper engagement with international partners. This global collaboration is proving essential in responding to increasingly sophisticated and transnational cyber threats.

Financial Sanctions Evasion

Rating

There has been an increase in sanctioned actors exploiting weaknesses in the global financial system through evolving tactics such as the use of virtual assets, obscured beneficial ownership, and intermediaries like shell companies and professional service providers. While Ireland enforces EU sanctions, these global vulnerabilities pose a low but growing threat, particularly in the context of complex financial sanctions evasion schemes.

Overview

In recent years, financial sanctions have been used as a significant foreign policy tool both by supranational organisations such as the UN and EU, and by national governments, including the United States, United Kingdom and others. The use of sanctions by differing authorities, under separate legislative regimes, and against different targets has resulted in a complex international sanctions framework. This complexity has substantially increased since 2022, following the wide-ranging sanctions imposed against Russia – including by the EU – as a result of its illegal invasion of Ukraine. The divergence in sanctions regimes, as well as the complexity of the international framework, create avenues for sanctions evasion that Ireland, despite its robust compliance with EU obligations, may be exposed to.

The Democratic People's Republic of Korea ("DPRK"), Iran and Russia have been identified as the state actors most heavily involved in sanctions circumvention activity. The EU and others are taking action to address sanctions circumvention, including through the introduction of new reporting requirements[95] which will assist in the identification of sanctions evasion activity in relation to Russian sanctions. As of December 2025, there have been eight cases of financial sanctions evasion reports, and a further 43 cases of self-reported breaches of EU sanctions submitted to the Central Bank. Of these 43 cases, 26 were submitted by entities in the funds sector, and the remaining were submitted by a combination of credit institutions and other sectors. There is therefore currently limited evidence of significant sanctions evasion activity with a nexus to Ireland.

[95] For example, Article 5r of Council Regulation No 833/2014

Financial Sanctions Evasion Threats

As the FATF's 2025 paper[96] outlines, there are three threats relevant to financial sanctions evasion: use of virtual assets, obscuring beneficial ownership, and enlisting intermediaries.

Use of Crypto Assets: As noted in the CASPs sectoral risk assessment, there has been significant growth in the crypto-assets industry in recent years, including in Ireland; the regulatory regime has also been and continues to be expanded for the sector. However, the sector presents vulnerabilities that may facilitate sanctions evasion. A recent FATF report highlighted that virtual assets are increasingly used to bypass sanctions, and that the DPRK had "generated billions of dollars through cyberattacks on virtual asset-related companies, such as the theft of $1.5 billion from ByBit in February 2025".[97]

Obscuring Beneficial Ownership: Sanctioned actors deliberately conceal the true ownership and control of assets to bypass sanctions and integrate into the legitimate financial system. This is often achieved through complex corporate structures, including the use of shell companies, nominee directors, and trusts across multiple jurisdictions, particularly those with weak transparency requirements. These structures are designed to create distance between the sanctioned individual or entity and the assets or transactions, making it difficult for financial institutions and authorities to identify the ultimate beneficial owner. This threat can exploit weaknesses in CDD frameworks, inconsistent global standards for beneficial ownership registers, and limited information-sharing between jurisdictions, all of which can hinder effective sanctions implementation and enforcement.[98]

Enlisting Intermediaries and Use of Front Companies: Sanctioned actors and proliferation networks also routinely enlist intermediaries, including brokers, lawyers and logistics providers, as well as front companies to mask their involvement and facilitate access to goods, services, and the financial system. These intermediaries are often based in jurisdictions with weak enforcement or limited sanctions and are used to create distance between the sanctioned individual or entity and the end transaction, and bypass sanctions controls such as screening. Ireland is exposed to this risk through its internationally active corporate service providers, trading firms, and financial institutions, which may unknowingly transact with or support intermediaries acting on behalf of sanctioned parties.

[96] FATF Report / Complex Proliferation Financing and Sanctions Evasion Schemes / Available from: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Complex-PF-Sanctions-Evasions-Schemes.pdf.coredownload.inline.pdf
[97] Ibid. / p. 6
[98] Ibid. / p.29 - 37

Bribery and Corruption

Rating

Bribery and corruption generate illicit proceeds through abuse of public or corporate positions, often linked to procurement-related offences. Ireland performs well in international corruption indices, albeit the scale of domestic corruption is difficult to gauge, and under-reporting does remain a concern. Most domestic cases involve low-value procurement-related offences, while international risks include Irish entities operating in high-risk jurisdictions. The use of digital tools and virtual assets to conceal corrupt payments is increasing, adding complexity to detection and enforcement. However, based on the low incidence of bribery and corruption, it is assessed as posing a low ML threat.

Overview

In Ireland, bribery and corruption are primarily defined and criminalised under the Criminal Justice (Corruption Offences) Act 2018. The term 'corrupt' is defined in this Act, and includes acting with an improper purpose personally, or a) by influencing another person by making a false or misleading claim, b) withholding, concealing, altering or destroying information or destroying a document or c) by other means. A 'bribe' is referred to as "a gift, consideration or advantage" to a person as an inducement to, or reward for, or otherwise on account of, any person doing an act in relation to his or her office, employment, position or business. A bribe can be given or received directly or indirectly, alone or with another person. The bribe does not need to be actually given or received, as offering, agreeing to give or requesting it are also specified as being offences under the Act.

Corruption is estimated to cost the EU between €179 billion and €990 billion each year, amounting to 6% of its GDP,[99] and is considered a critical enabler of organised crime globally, with almost 60% of criminal networks engaging in corruption.[100] As noted by Europol, bribery and corruption are integral elements of almost every organised criminal activity, and can range from petty bribery to complex multi-million-euro schemes. Due to the nature of corruption, there is presumed chronic under-reporting of corruption, which makes it difficult to accurately evaluate.[101]

[99] European Commission / Anti-corruption / https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/democracy-eu-citizenship-anti-corruption/anti-corruption_en
[100] Europol / Corruption / https://www.europol.europa.eu/crime-areas/corruption
[101] Europol / Serious and Organised Crime Threat Assessment / https://www.europol.europa.eu/cms/sites/default/files/documents/socta2021_1.pdf / p. 26

As noted by the IMF, the underlying mechanics of corruption have not changed in recent years, however, the use of technology has changed the mechanisms for committing and moving funds relating to bribery and corruption. For example, cryptocurrencies are increasingly used to make payments to corrupt officials, and digitalisation of the public sector will lead to the targeting of those in positions who can influence or manipulate processes and decisions in digital systems, or who can facilitate access to valuable digital data.[102]

From an Irish perspective, An Garda Síochána has estimated the total value of alleged bribery in open investigations to be approximately €40 million, however bribery and corruption are not always monetary in nature. While some forms – such as cash payments, free flights, or covered expenses – can be quantified, others are more difficult to value. Examples include preferential treatment, influence over decision-making, or access to confidential information. Ireland performs well in multiple international assessments in relation to corruption risk, being ranked 10th least corrupt on the Corruption Perceptions Index,[103] and the World Bank's 2023 Control of Corruption Index ranks Ireland in the 92nd percentile of countries in terms of effectiveness in controlling corruption. According to the World Bank Enterprise Surveys on Corruption, Ireland reports a bribery incidence rate of just 0.3%. This is significantly lower than the average for firms in Europe and Central Asia at 6.1%, and the global average of 11.2%.[104]

Law Enforcement Intelligence

Ireland faces exposure to foreign bribery and corruption risks, particularly involving Irish entities operating in the natural resources sector. Bribery and corruption schemes often use local intermediaries with no formal footprint in the host country to facilitate payments, with proceeds laundered through trade-based mechanisms. Investigations are frequently linked to jurisdictions which score poorly on internationally recognised bribery and corruption indices, and investigations can be hindered where information is being sought from countries with weak MLA frameworks.

Domestically, corruption cases tend to involve lower-value procurement-related offences, including cash bribes, preferential treatment, and corporate hospitality. As of December 2025, the Anti-Bribery and Corruption Unit ("ABCU") in the GNECB is managing fifteen active investigations, which includes four foreign bribery cases. A further five matters are under

[102] Ibid.
[103] Transparency International / Corruption Perceptions Index / https://www.transparency.org/en/cpi/2024
[104] https://www.enterprisesurveys.org/en/data/exploreeconomies/2024/ireland#corruption

assessment. Several cases were closed due to prosecutions abroad or insufficient evidence. The ODPP is considering one investigation file, and one person is currently before the courts charged with active corruption under the Criminal Justice (Corruption Offences) Act 2018.

Organised Crime Groups in Ireland

While Ireland does not have a significant number of OCGs compared to larger EU countries, those that do operate in the State are among the most significant in Europe. OCGs in Ireland are involved in a wide range of criminal enterprises, with some groups being highly sophisticated, violent, and internationally connected.

Irish OCGs are known to have defined organisational leadership systems, engage in a range of illicit activities, and are often influenced by family and kinship relations. As a result of law enforcement successes in tackling the most violent OCGs, there has been a significant downturn in OCG-related murders in recent years in Ireland.[105]

Case Study: International action against an Irish OCG

A notable example of Ireland's international cooperation in combating organised crime is the work undertaken with US and UK authorities against an Irish OCG. In April 2022, this resulted in the US Office of Foreign Assets Control designating key members and associated entities of the OCG, which blocked property and interests in property under U.S. jurisdiction and prohibited US persons from engaging in transactions with the designated individuals and entities.

The European Context

Organised crime profits from illicit activities in the nine main criminal markets in EU[106] amounted to €139 billion in 2019.[107] As of 2024, Europol identified 821 major transnational criminal networks active across the EU, and total membership of these organisations exceeds 25,000 individuals.[108] These groups are estimated to earn annual profits of between several million to tens of millions of euros each, with a select few generating up to €1 billion a year.[109] They operate in a wide range of criminal enterprises, including drug trafficking,

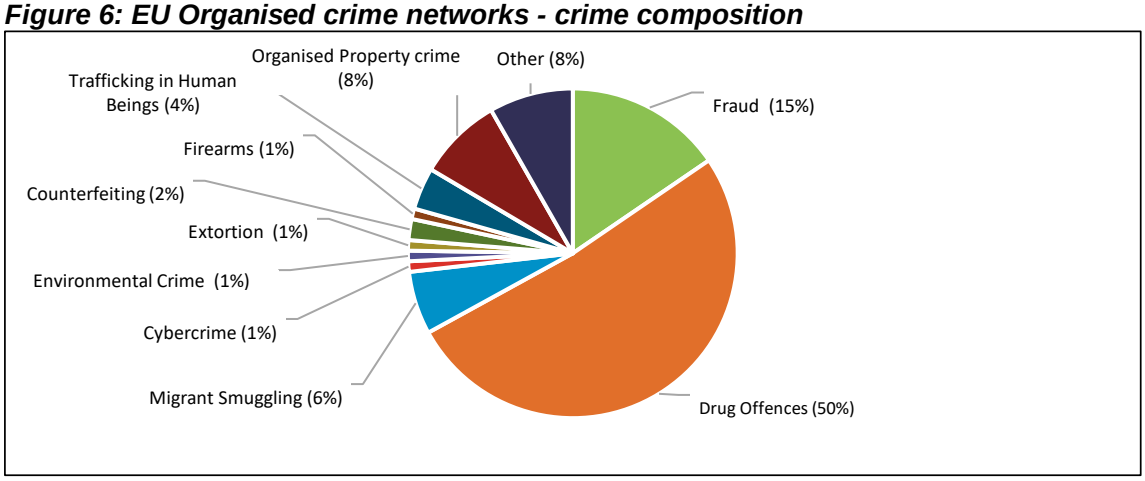
[105] Global Initiative Against Transnational Organized Crime / Global Organized Crime Index 2023 / Available from: https://ocindex.net/2023/country/ireland
[106] Illicit drugs, THB for sexual exploitation, smuggling of migrants, MTIC fraud, illicit waste, illicit firearms, illicit cigarettes, card payment fraud and cargo theft.
[107] European Commission / Mapping the risk of serious and organised crime infiltrating legitimate businesses 2021 / Available from: https://op.europa.eu/en/publication-detail/-/publication/ab3534a2-87a0-11eb-ac4c-01aa75ed71a1/language-en / p.15
[108] Decoding the EU's most threatening criminal networks / Available from: https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20report%20on%20Decoding%20the%20EU-s%20most%20threatening%20criminal%20networks.pdf / p. 9
[109] Decoding the EU's most threatening criminal networks / p. 55

fraud, migrant smuggling, human trafficking, organised property crime, and cybercrime. Half of the most significant groups are involved in drug trafficking.

The most threatening OCGs operate without borders, conducting transnational activities that span multiple countries. These networks are highly international, with members from across the EU and beyond collaborating to carry out complex, cross-border criminal operations. 68% of EU networks are composed of members from multiple nationalities, while 32% have members from only one country.[110]

Some 280 of the most threatening criminal networks in Europe have been active for 10+ years, and 86% of those use legal business structures, including to facilitate criminality, as fronts for the activity, and as vehicles to launder profits. Sectors such as construction, hospitality and logistics are noted as being most vulnerable to infiltration by OCGs.[111] The criminal activity profile of OCGs in Ireland closely aligns with the broader crime composition observed across the EU, as seen in the diagram below.[112]

Figure 6: EU Organised crime networks - crime composition



Money Laundering Techniques of OCGs

To obscure the origins of illicit proceeds, OCGs employ a range of sophisticated ML techniques, which often involve moving funds overseas. Europol has highlighted that OCGs frequently outsource parts of their operations, such as technical services or low-level

[110] Ibid. / p .12
[111] Ibid. / p.10
[112] Ibid. / p.9

execution, to external providers operating under a crime-as-a-service model.[113] This trend has been observed in Ireland, with notable examples including:

- Chinese laundering network in Dublin: A Chinese OCG provided ML services to Irish-based groups, charging a 9% fee to move funds internationally.[114]

- Use of Russian laundering networks: Irish OCGs have collaborated with Russian networks such as Smart and TGR, which channelled at least €2 million per month through cryptocurrency and asset conversion schemes. These networks have been sanctioned by the UK's National Crime Agency and the U.S. Office of Foreign Assets Control for facilitating transnational ML.[115]

Irish law enforcement has identified that IVTS, including hawala-type networks, are highly active and operating within Ireland, including on behalf of OCGs. The increasing international connectivity of Irish OCGs has resulted in an increasing use of such services, enabling the movement of substantial criminal proceeds across borders.

Drug Trafficking and International OCG Links

Europol has highlighted that the most threatening criminal networks operate borderless criminal enterprises with members from multiple countries cooperating across jurisdictions.[116] Reflecting this trend, Irish OCGs have well established connections with major drug cartels in South and Central America. These connections enable the importation of large quantities of cocaine and other illicit drugs into Europe, often through maritime routes. Recent developments have seen increased cooperation between Irish law enforcement and UAE authorities, particularly through MLA frameworks, enhancing Ireland's ability to target and disrupt these networks.[117]

[113] Ibid. / p.14
[114] Irish Times / Criminal Assets Bureau inquiry exposes underground 'banking' network / https://www.irishtimes.com/crime-law/2023/11/04/criminal-assets-bureau-inquiry-exposes-covert-banking-network/?utm
[115] Irish Examiner / Irish crime gangs used Russian networks to launder at least €2m a month /https://www.irishexaminer.com/news/courtandcrime/arid-41530961.html?utm
[116] Decoding the EU'S most Threatening Criminal Networks / p.12
[117] Statement from Minister McEntee on Organised Crime / Available from: https://www.gov.ie/en/department-of-justice-home-affairs-and-migration/press-releases/statement-from-minister-mcentee-on-organised-crime/

Technological Sophistication and Encrypted Communications

Encrypted communication platforms are widely used by OCGs across Europe to securely coordinate illicit activities. Europol highlights tools such as EncroChat and Sky ECC as central to these operations.[118]

In Ireland, similar patterns are evident with the use of 'Ghost', an encrypted communication platform, which was widely used by OCGs to securely coordinate illicit activities such as drug trafficking, ML, and violent crimes. The platform's infiltration was achieved through Operation Kraken in 2024, a coordinated effort led by Europol and Eurojust and involving law enforcement agencies from nine countries. In Ireland, the operation targeted four major OCGs operating primarily in Dublin and the eastern region. An Garda Síochána conducted 33 searches, resulting in the seizure of €15.2 million worth of drugs, €350,000 in cash, cryptocurrencies, and 42 Ghost-encrypted devices. Eleven individuals were arrested, and further investigations are ongoing. The dismantling of Ghost underscores the critical role of international collaboration in combating transnational organised crime and highlights the adaptability of OCGs in leveraging technology to facilitate their operations.[119]

Broader Criminal Enterprises

Outside of drug trafficking, both Irish and international OCGs are involved in a diverse range of illicit activities including human trafficking, labour exploitation, arms smuggling, fraud, and property crime in Ireland. For example, a Cork-based Slovakian-run recruitment agency was uncovered in 2021 as a front for human trafficking and forced labour. A Lithuanian OCG trafficked vulnerable individuals into Ireland to work as heroin couriers, with 65 victims identified across coordinated An Garda Síochána, PSNI and Europol operations in 2020.[120] Meanwhile, Vietnamese criminal networks have trafficked people specifically to grow cannabis in specialised indoor farms, with cases in Dublin and Galway where victims were smuggled in shipping containers and exploited on arrival in Ireland.[121]

OCGs also smuggle firearms from former Soviet states and other Eastern European countries, and there are concerns that recent conflicts in Ukraine, the Middle East and North

[118] Decoding the EU'S most Threatening Criminal Networks / p.48
[119] An Garda Síochána Publication / Available from: https://www.garda.ie/en/about-us/our-departments/office-of-corporate-communications/press-releases/2024/september/an-garda-siochana-play-prominent-role-in-global-coalition-of-law-enforcement-which-takes-down-new-criminal-communication-platform1.html?utm
[120] Irish Times / Heroin-smuggling and people-trafficking network targeted with 18 arrests / Available from: https://www.irishtimes.com/news/crime-and-law/heroin-smuggling-and-people-trafficking-network-targeted-with-18-arrests-1.4340190?utm
[121] Irish Times / Jail for Vietnamese men 'smuggled into Ireland to grow cannabis' / Available from: https://www.irishtimes.com/news/crime-and-law/courts/circuit-court/jail-for-vietnamese-men-smuggled-into-ireland-to-grow-cannabis-1.3455757

Africa have contributed to arms trafficking to Ireland.[122] West African fraud gangs, alongside firearms traffickers, play a significant role in the broader criminal landscape. Additionally, some armed robbery gangs operate across the country, generating substantial profits through their activities.

Law Enforcement Intelligence

Ireland is home to OCGs that rank among the most active, strategically sophisticated, and internationally connected in Europe. These groups operate across multiple jurisdictions, shifting from traditional European bases like Spain to Middle Eastern hubs such as the UAE, exploiting favourable legal and financial environments. Irish OCGs are structured, with defined leadership tiers and diversified criminal portfolios including drug trafficking, ML, human exploitation, and arms smuggling. There is increasing evidence they maintain links with terrorist-affiliated individuals, providing services such as laundering, trafficking and weapons supply.

Their laundering techniques are highly sophisticated, involving trade-based schemes, cryptocurrency, and IVTS, notably hawala networks operated by Chinese and Pakistani facilitators. There have been significant law enforcement successes against these groups in recent years, including €627 million in drug seizures, €34 million in cash, and 1,722 arrests since 2015. However, the technological agility, global reach, and financial scale of these groups continue to pose a significant threat.[123]

[122] Global Organized Crime Index / Ireland / https://ocindex.net/2021/country/ireland?utm
[123] Garda Press Release / Garda National Drugs and Organised Crime Bureau, 10 years of Keeping People Safe / Available from: https://www.garda.ie/en/about-us/our-departments/office-of-corporate-communications/press-releases/2025/march/an-garda-siochana-garda-national-drugs-and-organised-crime-bureau-10-years-of-keeping-people-safe-march-2025.html

Terrorist Financing Overview

A standalone TF threat assessment for Ireland was first published in March 2025[124] based on analysis carried out between 2022 and 2024. The TF threat assessment contained in this NRA is based on updated analysis, different sectoral classifications, and in line with a consistent methodology for ML and PF. According to the Global Terrorism Index 2025, Ireland is ranked 90th globally, reflecting a low impact from terrorism; the nature of potential terrorist activity and support in Ireland is such that a distinction must be made between the differing threats from domestic terrorism and international terrorism.

Domestic terrorist activity covers the threat from illegal paramilitary groups whose activities are driven by opposition to the constitutional status of Northern Ireland and whose primary operational objective is to conduct attacks on police officers and security forces in Northern Ireland and Great Britain.

International terrorism covers the threats arising in connection with violent extremism having its roots in other issues – the most prominent of which at present is Islamist-inspired terrorism connected with conflicts in the Middle East and North Africa.

The Offences against the State Acts 1939-1998 are the State's primary body of counter-terrorism legislation. Under the Offences against the State Act 1939, there are two means by which an organisation may be proscribed as unlawful for the purposes of that Act.

Firstly, an organisation which engages in any of the activities specified in section 18 of the 1939 Act is declared to be an unlawful organisation for the purposes of that Act. Such activities include, inter alia, raising or maintaining or attempting to raise or maintain a military or armed force in contravention of the Constitution.

Secondly, an organisation may be declared to be unlawful by way of Government order pursuant to section 19(1) of the 1939 Act where the Government are of the opinion that the organisation concerned is an unlawful organisation and ought, in the public interest, to be suppressed.

[124] Ireland Terrorist Financing Risk Assessment, March 2025 / Available from: https://www.amlcompliance.ie/wp-content/uploads/2025/04/Terrorist-Financing-Risk-Assessment.pdf

Only two such orders were made to date in 1939 and 1983 which suppress, respectively, the organisation styling itself the Irish Republican Army (also the IRA and Óglaigh na hÉireann) and the organisation styling itself the Irish National Liberation Army (also the INLA). It has been held by the Courts that labels such as "official", "real", or "provisional" are immaterial to whether a group comes within the relevant order.

However, it is important to note that section 5 of the Criminal Justice (Terrorist Offences) Act 2005, which was enacted with particular application to international terrorism, ensures that any organisation which engages in terrorist activity or terrorist-linked activity is an unlawful organisation within the meaning and for the purposes of the 1939 Act. This is the case whether the organisation is in or outside the State or whether the activity occurs in or outside the State.

Within both the domestic and international categories, a further distinction must be made between the assessed threat of an act of terrorism within Ireland and the risk of TF activity to support such an act, and the assessed risk of TF activity within Ireland which is aimed at the support of an act of terrorism outside Ireland. In addition, increasingly there are other actors that resist easy classification, including growing levels of concern about right-wing extremism. The key trend in this area is growing evidence of transnational links between hyper-nationalist movements, facilitated by a toxic online environment on non-mainstream social media platforms. International links between right-wing extremist groups are a matter of increasing concern.

Terrorist Financing Risks

Domestic

Assessment of the Risk of an Act of Terrorism

Irish 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[125] has delivered a stable peace that commands overwhelming cross-community support across the island of Ireland, certain groups, with very limited levels of support, remain intent on disrupting the progress which has been achieved.

[125] The Good Friday Agreement, also known as the Belfast Agreement, is a landmark set of two agreements made in 1998 which were instrumental in bringing an end to the ethno-nationalist civil conflict in Northern Ireland known as ‘The Troubles’. It is made up of the Multi-Party Agreement between most of Northern Ireland’s political parties, and the British-Irish Agreement between the British and Irish Governments. Amongst other reforms, it established a consociational power-sharing arrangement.

While the Provisional IRA declared a ceasefire in 1997, the stable peace which followed the ceasefire did not enjoy total support from those involved in violent activity. Some terrorist organisations continued their activities and new terrorist groups emerged.

Dissident groups operate on a 'whole-of-island' basis, with activities occurring in Ireland and Northern Ireland. While logistical support, planning and financing may occur in both jurisdictions, in general it is not the objective of these groups to carry out acts of terrorism in this State, although these domestic terrorists can also be involved in a range of criminal enterprises in this jurisdiction. For that reason, it is assessed that an attack in Ireland from this source is unlikely. The terrorist risk assessment for Ireland remains moderate. An Garda Síochána is responsible for assessing the threat level from terrorism and consults with the Defence Forces in doing so. The Garda Commissioner regularly updates the Minister on security matters, in accordance with section 62 of the Policing, Security, and Community Safety Act 2024.

The UK has determined that the threat to Northern Ireland from Northern Ireland-related terrorism is substantial, meaning that an attack is likely, with members of the security forces being the most likely targets. The threat level was reduced from 'severe' to 'substantial' in March 2024. There are a number of republican paramilitary groups with varying strength and capability and posing varying levels of threat. It is important also to understand the potential linkages between republican paramilitary groups and OCGs in the State. A relationship of friction and facilitation exists between OCGs and some domestic terrorist groups. Distinguishing the activities of such groups from OCGs can also be complex, with domestic terrorist groups often acting in an identical manner to OCGs. This can be seen through the 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. Involvement in criminal activity is often for the personal enrichment of the members of domestic terrorist groups rather than for the financing of terrorist aims and activities.

Assessment of Risk of Terrorist Financing

The financial costs of funding domestic terrorist acts – including those taking place in Northern Ireland and Great Britain – are relatively small for the most part. The material used in such acts can often be procured through the activists' own personal means or direct theft. On occasion, more sophisticated material may have to be procured, requiring access to funding.

In cases where greater funding may be required, 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,

the drug trade, etc. Counterfeiting of goods has also been used by some groups more recently. These funds may then be laundered through cash enterprises 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. Since most of these fundraising mechanisms are criminal activities in their own right, it can be the case that they are dealt with on the basis of the detection and prosecution of those specific crimes. Such detection and prosecution can have the effect of forestalling any effort by the activists to finance specific activity falling within the TF offence. The continuing success of An Garda Síochána over the years has significantly degraded the capacity of these republican paramilitary groups to finance their operations and it is considered that such groups do not have significant reserves. Instead, they rely on ongoing criminal activities for funding, together with the modest personal resources of the small number of people directly involved in their groups. Self-financed operations have consistently been detected, disrupted and prosecuted as attempted terrorist offenders. Wider efforts to finance domestic terrorist activity have proven self-defeating due to their criminal character.

International

Assessment of Threat from Terrorism

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 of continued instability in the Middle East, in particular. The major security concerns relate to the radicalising influences that travellers to conflict zones are exposed to, the security risks some individuals may pose on returning to their home countries, and the potential for attacks by persons who have not travelled to conflict zones but are inspired by groups such as ISIS.

In this respect, Ireland enjoys a relatively benign security environment, with no specific intelligence of a particular threat, but recognition that a potential threat may exist. It is assessed that the current risk of an attack in Ireland from this source is moderate.

The threat from international terrorism is kept under constant and active review by An Garda Síochána, who take into account a range of considerations, including developments in the international threat landscape. Key considerations in relation to the current threat from international terrorism include:

- The threat posed by returning fighters from conflict zones;
- The potential for lone actors to carry out an attack;

- The aggressive stance, terrorist operations and radicalising potential of Islamist terrorist groups;
- Persistent online Islamist propaganda and recruitment efforts across a number of platforms
- 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.

An Garda Síochána enjoys a very positive relationship with communities in Ireland from which individuals may be considered as being vulnerable to radicalisation or recruitment to 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. In addition, a number of individuals have been fatally injured in such areas of conflict.

Assessment of Risk of Terrorist Financing

There is the possibility, albeit currently assessed to be low, that Ireland could be used as a base from which attacks could be planned. Such incidents would be likely to cause extreme disruption in the short-term and possibly longer-term reputational damage to Ireland both as a safe and secure destination and as an international partner in the fight against terrorism. Accordingly, the threat is kept under constant review, and the current assessment of low risk reflects careful assessment of the risk actors within Ireland for support to activities outside Ireland.

The number 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. Ireland accordingly assesses the risk of TF from within Ireland's resident population to be lower than the risk in other jurisdictions with larger and less well integrated immigrant populations from regions of concern.

Overview of Terrorist Financing-Related Prosecutions in Ireland

In 2019, Ireland secured its first conviction for TF under its AML/CFT legislation, involving an individual found guilty of providing financial support to a terrorist organisation. This landmark

case demonstrated the effective application of Ireland's legal framework and enforcement capabilities, particularly through agencies such as An Garda Síochána and the ODPP. To date, there have been four prosecutions involving TF in Ireland. While related offences, such as ML and membership of a terrorist organisation, have resulted in the successful prosecutions, no further convictions solely for TF have been secured. In three of these cases, the funding method was fraud, with destination countries including Turkey, Syria, Iraq, and Central Asia.

Table 18: Completed prosecutions in Ireland involving alleged TF (2020 – 2024)

Case	Funding Method	Transaction Details	Destination(s)	Conviction Details
ODPP v Atilla Tasgin	Fraud	€35,000 was transferred via 16 transactions through a Payment Intermediary ("PI"). The structured use of this channel over several years (2013 – 2019) may indicate efforts to obscure the origin and purpose of funds, consistent with potential TF typologies.	Turkey (believed onward to Syria/Iraq)	Convicted of ML; sentenced to 27 months (9 suspended). No TF charge.
ODPP v Malika Yakubova	Fraud	€30,000 was transferred through 16 transactions via an E-Money Institution ("EMI"). While the total amount is relatively low, the use of an international EMI over an extended period may indicate attempts to obscure the origin and destination of funds. This typology reflects the potential for EMIs to be exploited for TF purposes, particularly where transaction patterns are structured to avoid detection and monitoring thresholds.	Belarus, Pakistan, Turkey, Uzbekistan	Convicted of ML; 15-month suspended sentence. No TF charge.
ODPP v Faizullah Nazar	Fraud	A €2,500 payment was sent to Istanbul, Turkey via a PI. The case relied on circumstantial evidence, with the jury asked to determine whether the funds were proceeds of criminal conduct.	Turkey	TF charges withdrawn; ML offence proceeded to trial and resulted in a directed acquittal
ODPP v Lisa Smith	Self-funded	A single €800 transfer was made via a PI. While modest in value, the case illustrates that TF does not require substantial sums.	Syria/Iraq	Convicted of terrorist group membership (ISIL); acquitted of TF charge.

International terrorist groups, often through publications on social media, provide advice that travellers to conflict zones require little money to participate. While they do advise on the purchase of certain types of personal equipment and clothing, these costs are minimal and, for the most part, intelligence indicates that such individuals fund their own travel. Similarly, the emerging trend in recent atrocities in Europe is towards attacks which require little specialised resources or logistical and financing support, with the net effect that such attacks appear to be largely self-financed, giving rise to little need for TF in the sense of a backer passing funds to a perpetrator.

Evolving and Emerging TF Threats

Intensifying Terrorist Propaganda and Evolving Demographic Trends

There is an increasing risk of online radicalisation and recruitment targeting minors and adults exploited by terrorist groups using alternative internet platforms and encrypted chat applications and requiring little to no financial backing. Their independence from formal networks makes traditional counter-terrorism tools, like financial monitoring, less effective. In August 2024, a 16-year-old in Galway carried out a knife attack after being radicalised online through extremist Islamist content, including ISIS propaganda. An Garda Síochána and Europol classified it as Ireland's first confirmed jihadist terrorist attack.

According to the Global Terrorism Index 2025, one in five persons arrested for terrorism in Europe is legally a minor. In terms of CFT measures, this trend may come with additional challenges as those young individuals are in many cases likely to rely on someone else's financial resources and to show even more proficiency in using opportunities offered by digital innovations. Of particular concern is the increasing use of gaming platforms to influence minors and adults to exploit the platforms to disseminate propaganda, recruit members, incite and engage in radicalisation activities, communicate and sometimes fundraise.[126]

Against the backdrop of the already visible trend regarding the lower age of radicalised individuals, the use of AI by terrorist groups might pose a particular risk in the recruitment and radicalisation of young people, including through more targeted and tailored propaganda.

[126] Comprehensive Update on Terrorist Financing Risks 2025 / Available from: https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/Comprehensive-Update-on-Terrorist-Financing-Risks-2025.pdf.coredownload.inline.pdf / p.112-113

Combined Use of TF Methods with Modern Technologies

The FATF has observed a growing trend in the integration of traditional methods, such as cash and hawala and other IVTS services, with emerging digital technologies and payment systems for TF purposes. The growing convergence of methods used to raise and move funds, for example, combining online fundraising in crypto-assets with the subsequent use of IVTS or cash couriers, amplifies the challenges associated with each individual technique. This blended approach merges the difficulties of detecting physical cross-border cash movements with the complexities of tracing sophisticated virtual transactions.[127] The nature of IVTS makes it difficult for law enforcement to identify, investigate, and prosecute related activity. While there have been no specific cases identified in Ireland to date, the risk remains present due to the opaque and decentralised nature of these systems.

Globally, the expansion in terrorist use of digital platforms is a growing concern. The use of digital methods in the form of electronic wallets, sale of prepaid mobile cards, and virtual assets is expected to continue and become even more pervasive and significant. Connected to the increasing use of virtual assets and progressive successes in tracing VA transactions, is the growing exploitation of obfuscation techniques (e.g., shared digital wallets, mixers, chain-hopping) as well as a shift towards the use of alternative virtual assets which are promoted as more private and secure.[128]

Another growing trend is the sophistication of document forgery with the use of digital innovation, including AI. The use of fake or stolen credentials and identification documents has already been observed across a broad spectrum of sectors vulnerable to TF misuse, such as opening bank accounts, accessing money value transfer services, and engaging with VASPs.[129]

Convergence with Criminal Activities

As noted in the section above on OCGs, there is growing concern that terrorist groups are increasingly benefiting from criminal activities as both a source of financing and logistical support. Various types of terrorist organisations, both domestically and internationally, have been reported to generate substantial revenues through illicit economic activities and criminal enterprises. In 2021, the FATF highlighted that the establishment of links with OCGs not only

[127] Ibid. / p.111
[128] Ibid. / p.112 - 113
[129] Ibid. / p.112 – 113

enables terrorist groups to secure funding but also facilitates access to restricted or illicit goods, such as weapons and forged documents, thereby expanding their operational capabilities.[130] The convergence between terrorists and OCGs is expected to persist, posing ongoing challenges for law enforcement and CFT frameworks.[131]

Right-Wing Extremism in Ireland

In addition to well-established extremist categories, there is a growing concern in Ireland relating to right-wing extremism. Irish far-right groups increasingly draw ideological and tactical influence from international actors, including British and American extremists, which has resulted in anti-immigration protests and arson attacks targeting migrant accommodation. This is facilitated by an online ecosystem, with platforms hosting radicalising content and nationalist conspiracy theories, as well as enabling coordination across borders. In addition, evidence has emerged of online fundraising activities,[132] often involving cryptocurrencies, by Irish far-right influencers. Europol's TE-SAT report further underscores the threat, noting the increasing use of online propaganda to radicalise and mobilise support.

While Ireland has not yet experienced a major right-wing terrorist attack and there are currently no right-wing extremist groups classified as terrorist organisations in Ireland, the risk is increasing, and the international connectivity of these groups amplifies their potential impact.

Gender Perspective

A gender-sensitive approach is required for accurately assessing TF risks and developing effective countermeasures. Gender-blind or biased assessments can lead to misinformed assumptions, such as underestimating the role of women in TF activities. Evidence from other regions shows that women have increasingly been used as financial facilitators, cash couriers, or intermediaries in online fundraising campaigns, often due to lower scrutiny or cultural assumptions.[133] From a domestic perspective, republican paramilitary groups in Ireland have historically exploited gender bias in their activities.

[130] FATF, Ethnically or Racially Motivated Terrorist Financing (2021) / Available from: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Ethnically-or-racially-motivated-terrorism-financing.pdf.coredownload.inline.pdf / p.20
[131] Comprehensive Update on Terrorist Financing Risks 2025 / p.114
[132] Europol / European Union Terrorism Situation and Trend Report 2020 / Available at: https://www.europol.europa.eu/cms/sites/default/files/documents/european_union_terrorism_situation_and_trend_report_te-sat_2020_0.pdf
[133] Financial Action Task Force/ Comprehensive Update on Terrorist Financing Risks / p.32 – 35

Proliferation Financing Overview

This assessment describes the PF threats relevant to Ireland, which have been assessed as low. PF is defined as set out in the introduction section.

A PF threat refers to designated persons and entities that have previously caused, or have the potential to evade, breach or exploit a failure to implement PF-related Targeted Financial Sanctions ("TFS") in the past, present or future.[134] Such a threat may also be caused by those persons or entities acting for or on behalf of designated persons or entities. The threat of evasion of financial sanctions is assessed as a predicate offence to ML and should be read alongside this section.

Iran and the Democratic People's Republic of Korea ("DPRK") remain the most significant PF threat actors, due to their ongoing efforts to develop WMD and circumvent international sanctions.[135]

Proliferation Financing Risks

Financial Sanctions Evasion Related to PF

While there have been no confirmed cases of related sanctions breaches in Ireland to date, the risk of PF financial sanctions evasion remains a relevant and evolving threat. States subject to PF sanctions (i.e. DPRK and Iran) continue to exploit vulnerabilities in the global financial system to obscure the origin, movement, and purpose of transactional activity. Ireland's exposure to this threat is shaped by its role as a financial hub and the complexity of international financial flows. Further analysis of this is covered in the financial sanctions evasion section.

Wider Proliferation Threats

Defining PF threat solely relating to the evasion or breaching of PF-related TFS does not cover risks associated with wider proliferation financing and proliferation activities, such as the raising of funds for PF, the use of intermediaries for PF activities, and the nexus to goods

[134] Financial Action Task Force / Guidance on Proliferation Financing Risk Assessment and Mitigation / Available from: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Proliferation-Financing-Risk-Assessment-Mitigation.pdf.coredownload.inline.pdf / p.11
[135] Complex Proliferation Financing and Sanctions Evasion Schemes / p.6

which can be used for proliferation purposes. Wider proliferation threats are generated from both 'Direct' and 'Indirect' means.

Direct Proliferation Threat: Threats involving the actual or attempted financing of proliferation-sensitive goods, technology, or funds intended for use in WMD programmes.[136]

Indirect Proliferation Threat: Threats or financial activities that support proliferation efforts through intermediaries, front companies, or complex supply chains that obscure the true origin, destination, or end-use of goods or funds.[137]

Assessment of Direct Proliferation Threat

Ireland faces a low risk of direct involvement in the transfer of proliferation-sensitive materials. Ireland has a negligible military industrial base and a limited domestic production capacity for goods or technology used in WMD programmes (although Ireland does produce some dual-use goods). Ireland also maintains strong commitments to international non-proliferation treaties and conventions, underpinned through domestic legislation.[138] Furthermore, robust export control and licensing regimes are enforced.

Trade data from the UN's Comtrade database[139] suggests there is either no trade or no 'reporting of goods' between Ireland and DPRK, and a limited trade relationship with Iran. Furthermore, Irish exports of military goods to the rest of the world remain extremely limited; the average annual Irish exports of "Arms and ammunition; parts and accessories thereof" from 2020 to 2024 were below $450,000, and in 2024 Irish exports in this category amounted to just $86,462. While dual-use goods cover a broader range of categories and represent more complex trade flows, direct exports of conventional arms from Ireland are negligible.

While the risk is low, Ireland has advanced scientific research capabilities, and access to some dual-use technologies, including precision machine tooling and IT solutions, which can be targeted by foreign actors seeking to acquire expertise or materials for illicit purposes. The risk of Irish academic collaboration, technology transfer, or the misuse of research funding, particularly in high-tech sectors such as biotechnology, advanced materials, and electronics to assist in proliferation activity remains limited. Notwithstanding this, Ireland's controls and export regulations are robust, continue to evolve in response to potential risks,

[136] Guide to Conducting Proliferation Risk Assessment 2024 / Available from: https://static.rusi.org/guide-to-conducting-proliferation-risk-assessment-2024.pdf?utm / p.20 – 21
[137] Ibid. / p.21
[138] Prohibition of Nuclear Weapons Act 2019
[139] United Nations / UN Comtrade Database

and remain underpinned by implementation of EU dual-use and military export control regulations. These controls include licensing requirements, end-use certification, and enforcement mechanisms aimed at preventing the misuse or diversion of such goods.

Ireland's geographic distance and lack of established trading relationships with known PF threat actors such as the DPRK and Iran further reduce the likelihood of direct procurement or end-use by sanctioned entities. However, there remains a risk of diversion, particularly through intermediary jurisdictions with less robust controls, where sanctioned actors may exploit transshipment hubs or front companies to obscure the true destination or end-user of dual-use goods. Irish exporters, particularly those engaged in exports of dual-use goods, must remain vigilant in conducting end-user due diligence checks and monitoring payments that could obscure the ultimate beneficiary or purpose.

Assessment of Indirect Proliferation Threat

Irish PF threats also stem from indirect channels. Like many peer countries, Ireland is integrated with the global financial system and is host to numerous financial institutions with international reach. As such, Ireland is exposed to potential abuse by proliferation networks seeking to raise, transfer, or obscure funds in support of WMD procurement activities.

Proliferation networks often rely on complex financial arrangements to support procurement activity, such as layering of funds and the use of front or shell companies to mask ultimate beneficiaries. These activities may not originate in Ireland but may transit through the Irish financial system via correspondent banking, investment vehicles, or structured finance products. As noted by the FATF, illicit actors "*use banks to open accounts, and to facilitate international wire transfers without raising red flags using correspondent banking relationships to access international financial markets indirectly*".[140] The use of false documentation to obfuscate beneficial ownership, and transactions involving jurisdictions with weaker compliance standards, can further complicate detection and disruption efforts.

The financing of proliferation may involve transactions that appear legitimate, such as routine payments for industrial equipment or IT services, but when matched against sanctions lists, lists of dual-use goods, and of known typologies, present higher risk indicators. As such, Ireland's exposure to indirect PF threats – like many other peer jurisdictions – is closely linked

[140] Complex Proliferation Financing Sanctions Evasion Schemes / p.30

to the opacity of global financial flows, the use of complex international supply chains, and the potential misuse of legitimate financial and corporate structures for illicit ends.

Ireland's participation in the EU single market, which allows for the free movement of goods and services between member states, also introduces risk, as proliferation-sensitive goods can be moved through the single market (including Ireland) and exported to a third country of concern from an EU Member State with weaker export controls. This highlights the importance of coordinated EU-wide enforcement and vigilance to prevent exploitation of internal market freedoms for proliferation purposes.

Evolving and Emerging Proliferation Financing Threats

There is increasing evidence that other nation-state actors – in particular Russia – are assisting DPRK and Iran to circumvent sanctions, including PF-related TFS. For instance, the DPRK has increasingly expanded its financial connectivity, notably through strategic partnerships such as the DPRK-Russia Comprehensive Strategic Partnership Treaty (2024), which commits to strengthening economic and banking ties between the two countries. DPRK revenue generation for the purposes of its proliferation programme is diverse, extending beyond traditional sectors to include illicit activities such as forgery, fraud, cyber-crime, crypto-assets, and trafficking in arms, drugs, and wildlife.[141] Recent reports also indicate that Ireland has been targeted by DPRK operatives using fake identities to secure remote IT roles, in part to fund the WMD programme.

Iran relies on militarised proxies and transnational criminal organisations to evade sanctions and generate revenue.[142] These networks exploit overseas businesspersons, foreign exchange houses, and financial intermediaries to facilitate oil smuggling, ML, and complex sanctions evasion schemes that may support Iran's missile and WMD programmes. Ireland's open financial system and maritime links expose it indirectly to these risks, particularly given reports of illicit oil smuggling activities via the 'shadow dark fleet' that the Irish Government is actively seeking to address through international legal frameworks.

[141] Ibid. / p.16
[142] Ibid. / p.17

Money Laundering Typologies

ML, TF, and PF are dynamic and adaptive processes, shaped by the evolving tactics of criminal and terrorist networks, and the vulnerabilities within financial and non-financial sectors. Understanding the typologies, common methods, patterns and emerging risks used to move illicit funds, and the high-risk factors that enable them, is essential for effective detection and prevention. These typologies range from the use of cash-intensive businesses and shell companies to trade-based laundering, TF through charitable organisations, and PF via deceptive trade practices. Similarly, high-risk factors such as geographic exposure, customer profiles, and weak regulatory environments create opportunities for these activities.

Typologies and vulnerabilities rarely operate in isolation. Instead, they often intersect and reinforce one another, creating complex risk environments that illicit actors exploit across multiple stages of ML, TF, and PF. For example, weak CDD can enable both the placement and layering of illicit funds, serving as a common vulnerability across ML, TF, and PF schemes. This chapter highlights how these risks interact across financial crime strategies, emphasising the need for a holistic, risk-based approach to effectively detect and disrupt these threats.

Structuring / Smurfing

Structuring, or smurfing, is a technique used to avoid detection by breaking large sums of illicit cash into smaller transactions kept below reporting thresholds. These are spread across multiple accounts or institutions using individuals known as smurfs. For ML, the aim is to integrate illegal funds into the financial system; for TF, it is to covertly move and assemble funds. Structuring is widely used in money mule networks to evade scrutiny.

Structuring is a key placement method in ML, often exploiting weaknesses in systems that rely on fixed transaction thresholds, and can be effectively mitigated through the use of risk-based and behavioural monitoring to detect such patterns. Structuring is effective for criminals and terrorist financiers due to its simplicity and speed, as well as the difficulty posed to financial institutions in identifying this activity, especially when combined with techniques like money muling.

Case Study: Structured Cash Deposits in Human Trafficking Proceeds

Victims of human trafficking were instructed to regularly deposit cash amounts ranging from €200 to €1,000 into multiple Irish bank accounts over periods of six months to two years. This pattern of structured deposits was used to conceal the origins of approximately €95,000 in criminal proceeds, which were ultimately transferred to Nigeria and used to purchase property. Once investigated, these assets were subsequently frozen by the High Court under MLA provisions.

Money Muling

Money muling processes often form a key component of ML and TF operations, enabling networks to move illicit funds (including cash) quickly and discreetly across borders and between financial institutions. Money mule operations rely on recruiting individuals to receive, transfer, or withdraw illicit funds through their personal[143] accounts at financial institutions (including banks and payment firms).

Money muling can operate on a large scale, either through highly organised structures with designated recruiters, handlers, and coordinators, or through decentralised models that rely on digital communication tools like encrypted messaging apps and social media platforms. This flexibility allows the network to manage hundreds or even thousands of individuals simultaneously, often without direct contact. Once involved, money mules can help to deposit and move money across accounts, and often internationally, dispersing and layering transactions to obscure their origin. These funds can be converted into other forms, such as cryptocurrencies or High Value Goods ("HVGs"), inhibiting the ability of law enforcement to trace and seize them. Integrated with other ML typologies such as the use of shell companies or trade-based schemes, mule networks offer speed, scale, and anonymity, making them a powerful tool for OCGs and a persistent threat to global financial systems.[144,145]

According to the 2024 FraudSMART Money Mules Survey, between 2021 and 2024, over €44 million was laundered in Ireland using money mules, and nearly 9,000 money mule cases were identified in Ireland.[146] Young people, temporary visa holders and people in vulnerable

[143] Although business accounts can also be used for this purpose, in most cases accounts are personal
[144] Money Muling / Available from: https://www.europol.europa.eu/crime-areas/forgery-of-money-and-means-of-payment/money-muling?utm
[145] Garda National Economic Crime Bureau / Money Muling / Available from: https://www.garda.ie/en/about-us/organised-serious-crime/garda-national-economic-crime-bureau/money-muling.html?utm
[146] Banking and Payments Federation Ireland / FraudSMART Money Mules Survey 2024 / Available from: https://bpfi.ie/publications/fraudsmart-money-mules-survey-2024/?utm

circumstances are particularly targeted for use in money mule schemes. The 2024 FraudSMART Money Mules Survey also found that 45% of people aged 18–24 said they or someone they know had been asked to use their bank account to transfer money, and 34% admitted they would consider doing so for a share of the funds.[147] While the amounts moved through these accounts vary, they typically range between €5,000 and €10,000 per case.[148]

Case Study: OCG & ML via Smishing and Money Mules

A large-scale OCG operation involved the use of money mules within a local community, with Irish bank accounts and ATM withdrawals being exploited. Criminals employed smishing techniques to deceive individuals into sharing their banking credentials. Each transaction ranged from €1,000 to €5,000 and involved 48 suspects. The illicit funds were retained and circulated within Ireland, ultimately leading to significant asset seizures and a notable disruption of the organised crime group at the community level.

Trade-Based Financial Crime

Trade-based financial crime refers to the misuse of the legitimate international trade system to move often significant illicit value across borders. This includes Trade-Based Money Laundering ("TBML"), Trade-Based Terrorist Financing ("TBTF"), and Trade-Based Proliferation Financing ("TBPF"). These methods exploit the complexity and volume of global trade to disguise the origin, movement, or use of funds or goods/services, making detection and enforcement particularly challenging. While each serves a different illicit objective, ML, TF, or PF, they rely on similar techniques such as fraudulent invoicing, misclassification of goods, fictitious trading, and the use of front companies.

- **TBML:** Criminals manipulate trade transactions, such as via over or under-invoicing, multiple invoicing, or misrepresenting goods, to move illicit funds across borders under the guise of legitimate trade. These schemes typically occur during the layering stage of ML and are difficult to detect due to the involvement of legitimate businesses and complex international supply chains.

- **TBTF:** Terrorist groups exploit trade channels to move value, often by purchasing goods abroad with illicit funds, shipping them to conflict zones, and selling them, frequently for

[147] FraudSMART Money Mules Survey 2024
[148] Ibid.

cash, to finance operations. These schemes often mirror TBML techniques and may involve legitimate firms, making them harder to identify.

- **TBPF:** Used primarily to evade international sanctions, TBPF involves acquiring and transferring dual-use goods, those with both civilian and military applications, through deceptive trade practices. This includes mislabelling goods, using front companies, and routing transactions through multiple jurisdictions to obscure the origin and destination. These schemes may support the proliferation of WMD and often appear as standard commercial activity, complicating enforcement efforts.

Case Study: Trade-Based Laundering & IVTS

An Garda Síochána uncovered a laundering scheme run by one individual using fraudulent identities to open multiple bank accounts across institutions. These accounts enabled a trade-based laundering model, where illicit cash – mainly from online fraud – was withdrawn and re-deposited into fresh accounts to obscure its origin.

Funds were used to pay legitimate overseas invoices via multiple small transfers, spaced over days and routed through different accounts using consistent references. This mimicked routine business activity and avoided detection. Once goods were shipped and sold abroad, the intermediary directed which overseas account received the proceeds, maintaining a global flow of funds.

In parallel, the individual ran an informal remittance service, using laundered funds in overseas accounts to send money abroad for clients, bypassing formal financial channels. Transactions were kept below thresholds and spread across accounts to avoid red flags, creating a façade of legitimate business while laundering criminal proceeds.

Cash

In Ireland and across the euro area, euro banknotes remain widely used, despite a steady decline in cash payments. The total value of banknotes in circulation continues to rise annually, a phenomenon the European Central Bank (“ECB”) refers to as the “paradox of banknotes”, where cash becomes used more heavily for value storage. This persistent

reliance on cash presents significant risks across ML, TF, and PF, primarily due to its anonymity, portability, and lack of traceability.[149]

ML: Cash-based laundering remains a persistent challenge in Ireland. While the use of cash in legitimate economic activity has declined, criminal networks continue to exploit traditional methods such as cash smuggling, cash-intensive businesses, and money mule operations. Legitimate channels, including financial institutions and payment service providers, are still being misused to introduce illicit funds into the system. Despite advances in digital payments and regulatory oversight, there is no clear evidence that OCGs are moving away from cash. Instead, they are increasingly combining cash-based laundering with more sophisticated techniques, including the use of virtual assets and cross-border transactions.

Cash washing involves converting small denominations into high-denomination banknotes, making illicit funds easier to move and hide. However, very large denomination banknotes such as €100 and €200 do not circulate commonly in Ireland. Both denominations are less likely to be accepted by retailers and more likely to be flagged as suspicious by Retail Banks and Credit Unions. As such cash washing is more likely to involve the conversion of smaller denominations into €20 and €50 notes. Irish authorities and international bodies like the FATF stress the importance of robust customer due diligence and monitoring large or suspicious cash transactions to mitigate these risks.

[149] European Commission / Commission Staff Working Document Accompanying the Document Report from the Commission to the European Parliament and the Council on the Assessment of the Risk of Money Laundering and Terrorist Financing Affecting the Internal Market and Relating to Cross-Border Activities / Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022SC0344 / p.12

The below case study highlights how cash-based services are vulnerable to money laundering. Criminals exploited ATM withdrawals linked to foreign accounts and placed large volumes of illicit cash into Irish bank accounts. The anonymity of cash, weak controls around cross-border activity, and limited real-time monitoring make these sectors attractive for laundering criminal proceeds.

Inbound Cash Laundering – ATM Withdrawals & Foreign Accounts

The GNECB received a report of suspected ML from a domestic financial institution. The report detailed that, over approximately one month, three bank cards issued by a foreign financial institution were used to withdraw a substantial sum, totalling over €260,000 in cash from the domestic financial institution's ATMs. An updated report from the financial institution identified an additional twelve foreign bank cards used during the same period for significant cash withdrawals. In total, during that approximate one-month period, the fifteen identified foreign cards withdrew a combined sum of over €730,000 in cash from the ATMs.

Further inquiries with the financial institution confirmed that an additional sum of over €1.7 million had been withdrawn in cash from their ATMs utilising a similar MO since 2021. Overall, there were in excess of 1500 successful transactions using foreign bank cards amounting to nearly €2.7 million in cash withdrawals. The source of these funds remains unknown. The large individual withdrawal amounts, and the pattern of activity, suggest a deliberate targeting of ATMs with higher withdrawal limits, indicative of a coordinated money laundering operation. This matter is still under investigation with a number of arrests made.

TF: Cash remains a versatile and preferred transfer mechanism for TF. It is used to raise, store, move, and spend funds for operational needs such as salaries, logistics, and support to terrorists and their families. Unlike ML, TF often involves funding from legitimate sources, including personal asset sales, donations from diaspora communities, and revenue from businesses with high cash turnover. Terrorist groups frequently operate in informal economies and exploit porous borders to move cash across jurisdictions using couriers, hawala transfers, concealed transport, or smuggling routes. This widespread use of cash complicates efforts to trace financial flows and identify beneficiaries, posing a persistent challenge for CFT efforts.[150]

[150] Comprehensive Update on Terrorist Financing Risks / Available from: https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/Comprehensive-Update-on-Terrorist-Financing-Risks-2025.pdf / p.23

PF: In the context of PF, cash can facilitate the evasion of sanctions and the procurement of sensitive goods or technologies. Sanctioned entities can use cash to bypass formal financial systems, fund purchases through front companies or brokers, and move value across borders via informal channels. Its liquidity and opacity make it ideal for concealing the origin and destination of funds, especially when combined with deceptive trade practices and complex supply chains. FATF[151] has identified cash as a critical vulnerability in PF schemes, particularly where financial institutions and customs authorities lack visibility into end-use and end-user information.

Article 80 of the incoming AML Regulation will bring in additional limits on the use of cash, with a €10,000 (or equivalent in other currencies) limit on single or linked transactions. The effective implementation of this requirement should inhibit the use of cash by criminals.

High-Risk Jurisdictions

High-risk jurisdictions significantly elevate both ML, TF, and PF risks, often due to weak frameworks for the prevention of ML, TF, and PF, poor enforcement, and limited transparency. These jurisdictions often lack effective legislative and regulatory oversight, beneficial ownership disclosure, and international cooperation mechanisms, including MLAs.

Criminals exploit such environments to obscure the origin and movement of illicit funds by routing transactions through entities or accounts in these jurisdictions, facilitating layering and integration of illicit funds. Similarly, those seeking to commit TF may use high-risk jurisdictions to raise, store, or transfer funds, particularly where regulatory oversight is minimal or where enforcement is weak. In some cases, terrorist organisations may operate businesses or fundraising networks in these jurisdictions or use them as transit points for moving funds to conflict zones or sanctioned entities. The combination of the lack of transparency, limited regulatory scrutiny, and political instability in some high-risk jurisdictions creates fertile ground for both ML and TF activities, undermining global financial integrity and security.

Complex Legal Structures

Shell companies are legal structures often lacking substantial operations or assets, which can be used to obscure the ownership and control of both illicit and legitimate funds. These structures are exploited not only for ML, but also for TF and PF purposes. They enable bad actors to create complex layers of ownership which hinder efforts to understand the beneficial

[151] Complex Proliferation Financing and Sanctions Evasion Schemes / p.18

owners of assets, and to trace the origin, destination, and purpose of funds. Shell companies can be established in high-risk jurisdictions with weaker transparency requirements, can obscure ownership through the use of nominee shareholders, the use of intermediaries, and opaque corporate structures. In the context of TF and PF, these arrangements facilitate the raising, storing, and movement of funds across borders, support to sanctioned entities, and the financing of dual-use goods, while shielding the true beneficial owners and those operating the schemes from scrutiny.

Informal Value Transfer Systems

IVTS is a method of sending money across borders outside of the formal financial system. These systems use networks of people and personal connections to transfer value, with operators in different locations settling accounts with each other at a later time rather than physically sending money with each transaction. Examples include traditional systems like hawala. Their operation outside the formal financial system means they fall outside the scope of regulatory oversight and AML/CFT controls.

Irish OCGs have used hawala / Fei ch'ien style IVTS to launder criminal proceeds, particularly from drug trafficking through trusted intermediaries and international counterparties. These operations are facilitated through laundering-as-a-service networks, which specialise in providing OCGs with access to established laundering infrastructure, such as hawala and other IVTS operators. These networks enable Irish OCGs to move large volumes of cash funds internationally while avoiding contact with AML/CFT controls in the regulated financial sector see case study: Transnational Laundering Network (2022–2025).

Crypto-Assets

The use of crypto-assets has significantly increased and become more mainstream over the last ten years. Crypto-assets were originally designed to be a payment instrument; however, their primary utility to date has been for speculative investment rather than for third-party payments. Criminal networks have adopted crypto-assets for third-party payments, and accordingly, the ML, TF, and PF risk is significantly heightened. This can be seen with the use of crypto-assets as a payment mechanism in ransomware payments, drug trafficking, and other illicit activities.

Law enforcement in Ireland has seen increased use of crypto-assets in criminal activity, as highlighted in the CAB's 2023 annual report, where it stated: "Through its investigations the Bureau has made a number of seizures of various forms of cryptocurrencies including Bitcoin

and Ethereum".[152] Globally, the criminal exploitation of crypto-assets has also expanded and evolved. Europol's recent SOCTA 2025 report notes that cryptocurrencies are increasingly used to launder money within the EU.

The scope of ML threats now includes 'offline' crimes, such as major white-collar offences, in addition to cybercrime and crimes specific to crypto-assets. Cybercriminals increasingly rely on ML techniques such as money mules and mixers while some contract professional money launderers, engaging in a crime-as-a-service collaboration, as highlighted by Europol. In an Irish context, CASPs authorised and regulated under MiCAR face the challenge of detecting and mitigating these sophisticated ML techniques as well as the risks posed by the use of such products outside regulated platforms.

As per the above, crypto-assets are increasingly being used as a means of preferred payment in crimes such as ransomware attacks, which are a growing threat internationally, with 5,635 publicly reported attacks globally in 2024, up from 5,223 in 2023. While ransomware payments may not always flow directly through Irish-regulated CASPs, these entities remain at risk of exposure through subsequent laundering or conversion activities. Crypto-assets may also be used to evade financial sanctions, including due to the difficulty in linking wallets to beneficiaries.

Irish law enforcement agencies have noted instances where crypto-assets have been used by criminals to acquire illicit goods online, and there remains an ongoing risk that the convergence between OCGs and terrorist actors could result in similar patterns being used to finance terrorism (for more details see section 4.2.11 of Ireland's TF risk assessment).[153]

[152] CAB / Annual Report 2023 / https://www.cab.ie/wp-content/uploads/2024/10/CAB-Annual-Report-2023-Final.pdf / p.15
[153] Ireland's Terrorist Financing Risk Assessment

Case Study: DPRK Cyber-attack

In 2024, the Lazarus group, a hacking group alleged to be operated by the North Korean state, orchestrated a major hack against a Japan-based cryptocurrency exchange, DMM Bitcoin, resulting in the theft of 4,502.9 Bitcoin, worth $308 million at the time of the attack.

The Lazarus group member who was posing as a recruiter on LinkedIn contacted an employee of Ginco, a Japan-based enterprise cryptocurrency wallet software company. The attacker sent a malicious Python script disguised as a pre-employment test, which was then copied onto the employee's personal GitHub page which was subsequently compromised.

The Lazarus group exploited the session cookie information of the compromised employee, gaining access to Ginco's unencrypted communications systems. The actors likely used this access to manipulate a legitimate transaction request by a DMM employee, resulting in the loss of the Bitcoin. The stolen funds ultimately moved to TraderTraitor-controlled wallets.

Intelligence suggests that Irish criminals and OCGs have tended not to use crypto-assets as a mechanism for the storage or transfer of value, due to high volatility and challenges in transferring crypto-assets into fiat currencies. However, with the move towards increased integration of crypto-assets into the global economy (for example, more widespread adoption), crypto-assets may become a more attractive option for storing value for criminals.

STR submissions from VASPs in Ireland increased year-on-year from 2021 to 2023. STRs reported to the FIU by VASPs surged from under 3% of all STRs in 2021 to 31% in 2022, and to 43% in 2023. The reasons for this rise are multi-faceted and can be explained in terms of increased suspicious activity within the sector, improved risk awareness and reporting culture by firms in the sector, as well as some examples of defensive and duplicated reporting practices, further amplified by the growth in activity. During this period one VASP was responsible for a significant number of reports due to the review of a backlog of investigations; many of these reports involved indicators of suspected financial crime.

VASPs submitted a total of 6,903 (3,604[154] STRs and 3,299 STReu[155]) in 2024 which equates to 11% of the overall STR figure, a considerable decrease from the 2023 figures. Of these only 511 had an Irish nexus (with others being classified as "non-EU reports", submitted to

[154] Designation is selected by the entity at registration
[155] STReu is a specific report, usually submitted by entities located in Ireland and passporting their services to other EU countries, where there is no nexus to Ireland. All 21,463 of these reports have been processed and disseminated to the relevant EU FIU.

multiple FIUs simultaneously). Of those cases which have been fully analysed, ≈47% were disseminated; ≈13% to law enforcement and ≈34% to other FIUs.

Professional Money Laundering Networks and Enablers

Criminals who generate illicit funds must launder them to enable spending and sustain their activities. While some self-launder, many outsource this to Professional ML Networks ("PMLNs"), structured, for-profit organisations that specialise in concealing the origin and movement of criminal proceeds. PMLNs often operate independently of the underlying criminal groups and serve a range of clients, including drug traffickers, fraud syndicates, and other OCGs.

These networks are composed of professional enablers, accountants, lawyers, and company service providers, who deliberately facilitate ML. By misusing their expertise and failing to meet professional or regulatory obligations, these enablers help disguise the nature, source, ownership, and destination of illicit funds. Their involvement adds sophistication and credibility to laundering schemes, making detection more difficult as outlined in the Accounting Services Providers (''ASPs'') and Legal Services Providers (''LSPs'') sections.

Increasingly, these networks also exploit inside facilitators, trusted individuals within financial institutions and other regulated firms (including gatekeepers) who abuse their access to enable ML. These complicit insiders pose a significant threat to the integrity of key sectors, as they can bypass internal controls, manipulate records, and delay detection efforts. As illustrated in the case study A below, such abuse can result in the laundering of substantial criminal proceeds while evading internal scrutiny.

In the Irish and broader EU context, PMLNs pose a significant threat due to the region's open financial systems, high volume of cross-border trade, and access to professional services. These networks exploit regulatory gaps, inconsistent enforcement across member states, and the complexity of international financial flows to move large volumes of illicit funds as illustrated in case study B below.

Case Study A: Inside Facilitator

In 2024, a Retail Bank employee was convicted for laundering over €100,000 for the Black Axe OCG. His insider access allowed him to open and manage mule accounts, bypass controls, and coordinate fund movements, demonstrating the critical role of internal facilitators in professional laundering networks.

The operation relied on a structured muling network, with over 70 accounts used to move illicit funds. Many mules were vulnerable individuals, recruited through social media or personal connections, often unaware of the legal risks.

Black Axe's involvement added a transnational layer, linking Irish laundering activity to global cyber fraud and financial crime. Operation Skein exposed a disciplined, scalable laundering infrastructure, highlighting the need for stronger insider risk controls, mule detection, and international cooperation.

Case Study B: Transnational Laundering Network (2022–2025)

Between 2022 and 2025, an Irish OCG operated one of Europe's most extensive professional ML networks. Europol and Spanish authorities uncovered a system that is suspected to have laundered over €200 million in a single year using a blend of hawala-style transfers, shell companies, and luxury goods to disguise the origin of criminal proceeds.

The network functioned as a "laundering-as-a-service" model, facilitating financial flows for multiple OCGs. It relied on professional enablers and complex corporate structures to integrate illicit funds into the legitimate economy. The cartel's laundering infrastructure spanned the EU and the Middle East, exploiting regulatory gaps and cross-border financial systems to move money discreetly and efficiently.

This case highlighted the scale, sophistication, and international reach of modern laundering operations, and the critical role of professional facilitators in enabling financial crime at a global level.

Case Study C: Trade-Based Money Laundering via Fraudulent Accounts

A financial investigation uncovered a sophisticated TBML scheme orchestrated by a single individual. Using fraudulent identity documents, the individual opened multiple bank accounts across various institutions, bypassing verification controls and establishing a broad financial footprint.

Illicit funds, primarily from online fraud, were withdrawn from one set of accounts and re-deposited into others, obscuring their origin. These funds were then used to pay legitimate invoices for overseas companies, simulating routine commercial activity. Payments were fragmented across multiple accounts and timed to avoid detection, with consistent invoice references used to mimic legitimate business practices. Following shipment of goods, the intermediary directed proceeds to designated overseas accounts, maintaining an international flow of funds. In parallel, the individual operated an informal remittance service, using laundered funds to send local currency equivalents abroad without engaging formal financial systems. The operation was carefully structured to mimic legitimate trade, conceal illicit flows, and avoid financial red flags.

Transnational Financial Flows

Transnational (cross-border) financial flows are a feature of Ireland's economy and financial sector given it is an open and highly interconnected economy with a moderately outsized financial centre.

The 2022 IMF Financial Sector Assessment Programme ("FSAP") for Ireland[156] underscored the necessity for improved cross-border data collection and advanced analytics to enhance the supervision of financial sector firms. This recommendation was reiterated in the 2025 IMF Article IV Report,[157] which emphasised the importance of adequately resourcing AML/CFT capacity. In response, the Central Bank has undertaken an examination of cross-border activities by regulated financial firms, focusing on identifying patterns and comparing these activities to trade and investment relationships. This analysis aims to screen for potential ML and TF risks at a population level, thereby enhancing the overall understanding of vulnerabilities within the financial sector.

The geographical analysis revealed limited connections to high-risk jurisdictions identified by the FATF or EU as having deficient AML/CFT regimes. However, there were somewhat elevated financial connections to offshore financial centres, which is expected given the international nature of certain segments of Ireland's financial services industry. Notably, the Irish financial sector is disproportionately linked to EU/EEA countries, where Irish firms provide services on a passporting basis, allowing them to operate across borders with relative ease. This enhanced geographical analysis is being integrated into the risk assessment of firms and sectors, informing the development of the Central Bank's supervisory strategy on an ongoing basis.

This analytical approach is being enhanced by now requiring regulated firms to supply transactional data by geography, specifically volumes and values of financial flows by country or territory. Enhanced regulatory returns are being phased in through 2025 and 2026 that will collect transaction activity by jurisdiction and increase understanding of risk exposures. This will enable much more precise risk analysis at both the sector and firm level, allowing for a more nuanced understanding of potential vulnerabilities. The implementation of these

[156] International Monetary Fund / Ireland: Financial System Stability Assessment / Available from: https://www.imf.org/en/Publications/CR/Issues/2022/07/07/Ireland-Financial-System-Stability-Assessment-520469
[157] International Monetary Fund / Ireland: 2025 Article IV Consultation-Press Release; Staff Report; and Statement by the Executive Director for Ireland / 2025 / Available from: https://www.imf.org/en/Publications/CR/Issues/2025/06/10/Ireland-2025-Article-IV-Consultation-Press-Release-Staff-Report-and-Statement-by-the-567588

enhanced returns is expected to significantly improve the Central Bank's ability to monitor and mitigate ML and TF risks effectively.

Additionally, the Central Bank continues to monitor transnational financial flows. In 2024, the Central Bank carried out a thematic review of transaction monitoring of cross-border payments by a sample of large firms. In terms of control weaknesses, the findings suggested some deficiencies in transaction monitoring systems and governance across sectors. Risk understanding and calibration of rules to assess risk also showed shortcomings which varied by sector. The findings demonstrate the need for firms to continually strengthen governance and improve updates of high-risk jurisdictions in order to address such weaknesses. This has been an area of continued focus for the Central Bank in its supervisory activities.

In addition, Ireland discontinued the Immigrant Investor Programme to new applications in 2023. This decision reflects concerns raised by the European Commission, Council of Europe and OECD regarding ML, tax evasion and border security associated with such schemes.[158] Its closure reduces the ML threat to these programmes and complements broader measures to strengthen Ireland’s AML/CFT/CPF frameworks in the context of transnational financial flows.

Ultimately, these initiatives aim to strengthen Ireland's AML/CFT frameworks and enhance the resilience of its financial system against transnational ML and TF threats, contributing to global efforts in combating financial crime and ensuring compliance with international standards.

[158] Department of Justice, Home Affairs and Migration / Available from: https://www.irishimmigration.ie/faqs-closure-of-the-immigrant-investor-programme-iip/ p.

Financial Services

Ireland's financial services sector is comprised of two broadly distinct parts. The first comprises well-established firms that provide banking, payments, and insurance services to domestic consumers and firms. The second largely comprises firms which provide higher-value services to customers outside Ireland on a cross-border basis. The latter are often foreign-owned, and their activities are tilted toward non-retail customers, including banking, payments, reinsurance, investment services, and funds management. Credit and financial institutions as defined in the CJA, operating within the financial services sector, whether domestically focused or internationally oriented, are 'designated persons' under the CJA and are supervised by the Central Bank.

The financial sector (both domestic and export-focused) employed 125,000 workers in 2024, accounting for 4.5% of total employment. Economic activity for the sector as measured by gross value added ("GVA") comprised €27 billion in 2024, about 5% of total GVA.[159] Ireland also ranks among the top five exporters of financial services in the EU and has been identified by the IMF as one of 29 jurisdictions with systemically important financial sectors. Taken together, these indicators suggest that Ireland has a moderately outsized financial sector.

In this context, five financial services sectors were selected for in-depth assessment due to their scale, complexity, and exposure to ML, TF, and PF risks. These sectors are:

- Retail Banks
- Non-Retail Banks ("NRBs")
- Funds
- VASPs
- PIs/EMIs

Each of these sectors was assessed using a consistent methodology that draws on a combination of qualitative and quantitative data to evaluate its exposure to ML, TF, and PF risks. Sources included regulatory returns, supervisory assessments, publicly available data, and insights from law enforcement, Government bodies, industry stakeholders, and individual firms. International guidance – such as from the FATF, the EU Supranational Risk Assessment ("SNRA"), and other relevant bodies – was also considered.

[159] Gross value added (GVA) is a measure of national economic activity defined as output (at basic prices) minus intermediate consumption (at purchaser prices). It is often used to look at economic activity by economic sector. Based on gross value added, income, and employment by detailed industry (NACE R2) [nama_10_a64] and [nama_10_a64_e]. NACE_R2 Code K for financial and insurance activities is used as a measure of the financial sector.

In addition to these five in-depth assessments, separate higher-level reviews were conducted for seven other financial services sectors. These reviews focused on identifying key risk indicators and sector-specific vulnerabilities, with a view to informing future prioritisation and supervisory engagement. The seven sectors are:

- Retail Credit Firms
- Bureaux de Change
- Life Insurance
- MiFID Investment Firms
- MiFID Markets Firms
- Retail intermediaries
- High-Cost Credit Providers

Retail Banking

Executive Summary

	2019 Risk Ratings	2026 Risk Ratings
Traditional Retail Banks		
ML	High	Very Significant
TF	High	Very Significant
PF	Not Assessed	Low
Digital Banks		
ML	Not Assessed	Very Significant
TF	Not Assessed	Very Significant
PF	Not Assessed	Low
Credit Unions		
ML	Medium-Low	Moderate
TF	Medium-Low	Moderate
PF	Not Assessed	Low

Key Insights

The heightened ML and TF risks for Traditional Retail Banks and Digital Banks largely stem from the scale and widespread use of their services, including a larger and more varied customer base, a broad product offering, and their greater international reach as compared to Credit Unions ("CUs"). In contrast, CUs, which operate within a limited and often localised market with less complex products and services, serve only their members, and this membership-based structure significantly reduces their exposure to ML and TF. Both Traditional Retail Banks and CUs are susceptible for placement of illicit funds in cash given their traditional branch model. In response, firms in the Retail Banking sector have made substantial investments in their ML, TF, and PF control frameworks, and many firms have well embedded controls, although Digital Banks may present certain operational and compliance challenges.

Retail Banks could be used to breach PF sanctions, although this risk is assessed to be low in an Irish context, due to the lack of direct transactional activity with jurisdictions of PF concern. Nonetheless, Retail Banks may have indirect exposure, including through correspondent relationships or transactions routed via higher-risk jurisdictions, which warrants continued monitoring and risk-based controls.

The key vulnerabilities in the sector are:

- **Widespread Availability and Sector Footprint:** Retail Banking's scale, accessibility, and central role in the financial system make it attractive and susceptible for ML and TF.

- **Control gaps in Retail Banking Sector:** Retail Banking services serve as key gateways to both domestic and international financial systems. As such, control gaps within firms in this sector can significantly amplify ML and TF risks, undermining market integrity.

- **Cross-border transactions:** Some Retail Banking products and services permit customers to conduct international transactions, including to higher risk jurisdictions and/or those with lower regulatory standards.

- **Cash:** Despite the shift towards digital transactions, cash is a significant vulnerability in Ireland's financial system. Due to its anonymity, accessibility, and widespread acceptance, cash remains a preferred method for holding and transferring criminal and terrorist funds.

- **Implementation of instant payments:** The growing shift toward instant payments poses ML and TF risks to Retail Banks, particularly in conducting effective 'real-time' transaction monitoring.

Defining the Retail Banking Sector

Retail Banking is central to the Irish financial system, serving as the primary gateway to financial services for individuals and businesses. It facilitates essential economic activities such as household payments, payroll, vendor transactions, and capital financing. The sector offers a comprehensive suite of services including current and savings accounts, lending and investment products, and payment services. Larger domestic Retail Banks also provide wholesale banking services such as correspondent banking and trade finance.

Retail Banks' services are used by virtually every household in Ireland, and every other sector is in some way affiliated with the banking system. This interconnectedness with both financial and non-financial sectors underscores the sector's materiality and criticality. Given its central role, and the attractiveness and widespread availability of its services, the banking sector is exposed to the broadest range of ML, TF, and PF risks.

The Retail Banking sector in Ireland is composed of:

1. **Traditional Retail Banks:** These are the three long-established Retail Banks, which offer a wide range of products to the public both via branch networks and increasingly through online banking channels. These institutions hold the majority of the local market share in terms of assets, loans and deposits.

2. **Digital Banks:** These are the digital-only banks, often offering specific features, such as P2P payments, rather than full-service banking, almost exclusively through non-face-to-face channels. These financial institutions are often established in Ireland as a Branch of a financial institution authorised in another EEA Member State. Currently, a broad range of services is offered through Freedom of Service ("FOS") via these Digital Banks, and this area is expected to grow as new entrants aim to compete directly with Retail Banks.

3. **Credit Unions:** These are generally local community-based or occupational-based institutions, established by and owned by members to serve on a not-for-profit basis. Recent legislative changes[160] have widened the scope of the products and services CUs can offer. A number of larger, consolidated Credit Unions have also emerged, enabling broader branch networks and expanded common bond areas, positioning them to compete more directly with Retail Banks.

Scale and Structure of the Retail Banking Sector in Ireland

The Irish Retail Banking sector is used by the vast majority of the domestic population, and processes high volumes of transactions through a variety of channels, including face-to-face, electronic payments and ATMs. As of mid-2024, the Retail Banking sector has approximately 14.3 million customers, of which 10.7 million are in Traditional Retail Banks and Digital Banks,[161] and 3.6 million in CUs. Irish consumers and SMEs are increasingly developing secondary relationships with Digital Banks and non-banks,[162] with 66% now using more than one banking provider, up from 57% in 2023.[163]

Two of the Traditional Retail Banks announced their intention to leave the Irish market in 2021, leaving just three such banks operating in 2025; the branch network has also been

[160] Exciting Times Ahead for Ireland's Credit Unions / Available from: https://www.gov.ie/en/department-of-finance/press-releases/exciting-times-ahead-for-irelands-credit-unions/
[161] Central Bank of Ireland data
[162] Department of Finance / Retail Banking Review / Available from: https://assets.gov.ie/static/documents/retail-banking-review-november-2022.pdf / p.63
[163] Department of Finance / Consumer Sentiment Banking Survey August 2024 / Available from: https://assets.gov.ie/static/documents/consumer-sentiment-banking-survey-report-2024.pdf / p. 4

reduced, dropping from 617 branches in June 2020 to 438 in September 2022,[164] and further in 2024 to 432 branches[165] driven by institutions increasingly shifting towards digital-first operating models. This shift reflects growing demand for flexibility and digital convenience. In 2022 alone, contactless payments reached nearly €17.9 billion, a 31.4% increase from the previous year.[166] Meanwhile, Ireland's largest Digital Bank is estimated to have established a relationship with approximately 39% of Irish residents, up from 18% in 2022;[167] however, only 3% currently use it as their main current account.[168] Irish customers more typically use Digital Banks for specific features, such as P2P payments, rather than full-service banking. This is expected to change as Digital Banks continue to expand their offerings and seek to build consumer trust.

The number of CUs has decreased[169] from 227 in February 2022[170] to 174 in December 2025.[171] The Irish League of Credit Unions, representing 90% of active Irish CUs, reported that in 2024, CUs processed over 32 million electronic payments, 17% more than 2023, with 59% contactless. Digital transactions hit €2.3 billion, up 28% year-on-year.[172]

The majority of customers of Irish Retail Banks are domestic, with many having a long relationship with the same bank, although a wide variety of products and services are offered to non-residents. Traditional Retail Banks operate through extensive countrywide branch networks, with these 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. While there are eight Retail and Digital Banks in Ireland, the sector in Ireland is dominated by the three Traditional Retail Banks,[173] on which Irish customers continue to rely for their key banking services. In addition, a state-owned financial and postal services provider (classified as a Retail Bank for the purpose of this assessment), provides a similar set of products and services as Retail Banks, including through its nationwide network of 892 branches.

[164] Department of Finance / Retail Banking Review / p.64
[165] Central Bank of Ireland data
[166] Banking and Payments Federation Ireland / Payments Monitor Q4 2022 / Available from: https://bpfi.ie/publications/bpfi-payments-monitor-q4-2022/
[167] Consumer Sentiment Banking Survey August 2024 / p.4
[168] Ibid. / p.4
[169] Attributable to transfers of engagement in the Credit Union market. A Transfer of Engagements refers to the legal process by which one Credit Union transfers all its assets, liabilities, and members to another Credit Union. This typically results in the merging of two or more Credit Unions into a single, larger entity.
[170] Central Bank of Ireland data
[171] Central Bank of Ireland data
[172] Credit Union / Q1 FY2025 Quarterly Results / Available from: https://www.creditunion.ie/news/latest-news/q1-fy2025-quarterly-results-show-continued-growth/
[173] Consumer Sentiment Banking Survey August 2024 / p.16

Entities within the PI/EMI sector also offer a similar set of products and services as Retail Banks, such as payment accounts, debit cards, ATM access, direct debits, and mobile payments. While not licensed as banks, these providers compete with Retail Banks and deliver comparable functionality for everyday transactions. This shift reflects a broader transformation in Ireland's financial ecosystem, where technology-driven, non-bank institutions are stepping in to compete and fill service gaps, particularly as the traditional banking sector consolidates and physical branches close.

Threats and Vulnerabilities

Threats

The ML, TF, and PF threats to which Ireland is exposed are assessed above. Due to its key role as an entry point to the financial sector, the Retail Banking sector faces heightened exposure to several threats, including the placement of the proceeds of crime into the financial system. Deposits on account, in particular, are used by OCGs as it is one of the easiest mechanisms for integrating illicit funds (including cash) into the financial sector. Law enforcement has also identified cases of professional ML operations (including those based overseas) in establishing complex ML operations using Retail Banking products; less sophisticated mechanisms, such as the use of money mules, are also a key ML typology in the sector. Globally, Retail Banking products, particularly current accounts, are frequently used by terrorists and their supporters, friends and family to facilitate TF.[174] According to information from competent authorities, terrorists withdraw funds from bank accounts via ATMs located in high-risk non-EU countries, conflict zones, or neighbouring countries (for more details see section 4.2.1 of Ireland's TF risk assessment). In addition, the scale and interconnectedness of the Irish financial system mean that the proceeds of some foreign illicit activities may enter or pass through the Irish Retail Banking sector.

A total of 25,375 STRs (21,668 submitted by Retail Banks and 3,707 submitted by CUs) were submitted by firms in this sector in 2024. Approximately 14% of the analysed STRs were disseminated; ≈11% to law enforcement, and ≈3% were disseminated to other FIUs. ML was cited in 88% of the total STRs submitted in 2024.[175]

[174] European Commission (2022) / Commission Staff Working Document Accompanying the Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities / p.38

[175] Due to differences in how entities are categorised within this sectoral risk assessment, FIU Ireland manually compiled the data presented in this section. It should be noted that the analysis provided shows a single classification for each individual STR. However, an STR can be sent to multiple jurisdictions resulting in multiple disseminations. The figures contained in this

Vulnerabilities

Vulnerability 1: Widespread Availability and Sector Footprint

The widespread availability and usage of Retail Banking products (as noted in the 'scale and structure' section above), combined with the sector's systemic role within the financial system, increase its exposure to ML and TF activities. Retail Banking serves as a primary gateway into the financial system, with products that are both essential for legitimate financial activity and susceptible to criminal misuse.

The sector offers a broad array of financial products, some of which, such as personal current accounts, are particularly attractive for illicit purposes. These accounts can facilitate the deposit of cash, enable international transactions, and support the rapid movement of funds through instant payments. Their accessibility to all customer types, including higher-risk individuals such as PEPs, further elevates the risk. Notably, 95% of Retail Banks and 75% of CUs report having PEPs within their customer base.[176]

Following the 2021 announcements by two Traditional Retail Banks of their planned exits from the Irish market, only three such banks remain operational as of 2026. There was a significant surge in account openings, with 1,200,810 new current and deposit accounts opened by mid-2023, 801,648 of which were current accounts.[177] The transfer of the customer base led to a notable improvement in the quality of customer information and associated risk profiles. All customers were required to provide up-to-date Know Your Customer ("KYC") documentation during the onboarding process, information that may have previously been outdated or incomplete in their former banking relationships.

The combination of product availability and the sector's extensive footprint makes Retail Banking particularly susceptible to exploitation, and common ML typologies can be facilitated through these products. For example, in Ireland approximately €9.4 million was laundered through money mule accounts in the 12 months to June 2025.[178] This risk is especially

report do not reflect multiple disseminations. Furthermore, where an STR is classified as disseminated to Law Enforcement or another FIU it is not further classified by crime type.

[176] Central Bank of Ireland data

[177] Account Migration Statistics / Available from: https://www.centralbank.ie/docs/default-source/statistics/data-and-analysis/credit-and-banking-statistics/account-migration-project/account-migration-statistical-release.pdf?sfvrsn=136c9b1d_5

[178] Banking and Payments Federation Ireland / Almost €9.4m laundered through money mule accounts / Available from: https://bpfi.ie/money-mules-2025/

concentrated among younger customers, particularly those aged 18–34, who are often recruited via social media and messaging platforms in exchange for money or gifts.[179]

The nature of the products and the scale, accessibility, and systemic importance of the Retail Banking sector, collectively create a high-risk environment for financial crime.

Case Study: Money muling

In 2024, Gardaí in County Kerry uncovered a large-scale ML operation involving the movement of over €1.3 million through the bank accounts of young people, many of whom were still in school. The operation revealed that individuals aged between 16 and 20 were being recruited via social media platforms to act as money mules, allowing their bank accounts to be used to transfer illicit funds. In exchange, they were promised a small percentage of the laundered money, typically around 10–15%.

As a result of the investigation, 32 individuals were prosecuted in both District and Circuit Courts, with some accounts found to have processed up to €65,000.

Vulnerability 2: Control Gaps in Retail Banks

Traditional Retail Banks in Ireland generally operate with mature AML/CFT/CPF frameworks. These frameworks have been subject to regular supervisory assessments by the Central Bank, which has not identified significant deficiencies in recent years. However, as these institutions increasingly adopt instant payments and seek to enhance their customer experience to align with offerings from Digital Banks and PI/EMI competitors, vulnerabilities may emerge. In particular, the shift toward faster, technology-driven processes may, in some cases, lead to inconsistent application of CDD and risk assessment methodologies.

This challenge is particularly pronounced for Digital Banks, where rapid growth and increasing market share in Ireland have intensified operational pressures. The expectation of seamless, near-instant onboarding at scale places significant strain on CDD frameworks. This heightens the risk that key controls may be bypassed, inconsistently applied, or deprioritised in favour of customer experience. Examples of potential control weaknesses observed in the sector internationally (though not specifically identified in Ireland) include

[179] Garda National Economic Crime Bureau / Money Muling / Available from: https://www.garda.ie/en/about-us/organised-serious-crime/garda-national-economic-crime-bureau/money-muling.html#:~:text=Newcomers%20to%20the%20country%20(often,compared%20to%20people%20aged%2055%2B

instances where Digital Banks operating in Ireland failed to conduct adequate levels of CDD and monitoring.[180]

CUs are generally rated as lower risk than Traditional Retail Banks by the Central Bank, reflecting their community-based business models, smaller set of products and services and lower usage and adoption in the market. However, the emergence of larger CUs adopting branch-based structures and expanding operations has introduced new complexities.[181] In this context, the voluntary ethos of the CU movement should also be considered a potential challenge, particularly from a compliance culture and control framework maturity standpoint. While all CUs are overseen by volunteer boards and operate within community/industry-based decision-making structures, this model may constrain the pace and depth of progress in embedding more robust governance, risk management, and compliance frameworks. As these institutions scale, their operational controls and transaction monitoring and screening systems may not yet match the maturity or robustness seen in other parts of the Retail Banking sector, potentially creating vulnerabilities.

Where CDD and monitoring processes are weak or inconsistently applied, criminals are likely to exploit these gaps using ML typologies. If there are systemic failures in the CDD and monitoring processes of a single Retail Bank, the impact can ripple across the financial system, undermining the integrity and trust of the broader financial services ecosystem.

The products and services offered by the Retail Banking sector will continue to be attractive to bad actors and for use in ML and TF operations. The external risks faced by the regulated sectors are not static, with criminals constantly evolving their techniques to use the financial system to launder the proceeds of crime or fund terrorism. Therefore, it is key that the entities that make up the Retail Banking sector ensure they maintain a robust understanding of the risks they face, and that they keep improving their controls to address new and emerging risks and typologies.

[180] Irish Times / Revolut fined €3.5m by Lithuanian Regulator 2025 / Available from: https://www.irishtimes.com/business/2025/04/08/revolut-fined-35m-by-over-money-laundering-control-failures/ & RTE / N26 Suspicious Transaction Reporting Control Failures 2024 / Available from: https://www.rte.ie/news/business/2024/0528/1451687-german-online-bank-n26/
[181] Central Bank of Ireland data

Vulnerability 3: Cross-Border Transactions

According to the Payment Statistics Quarterly,[182,183] total transaction volumes of non-cash transactions continued to rise in the first half of 2025. Credit transfers alone reached 499 million transactions, up from 446 million in the first half of 2024, with their total value increasing from €5.3 trillion to €5.7 trillion year-on-year.

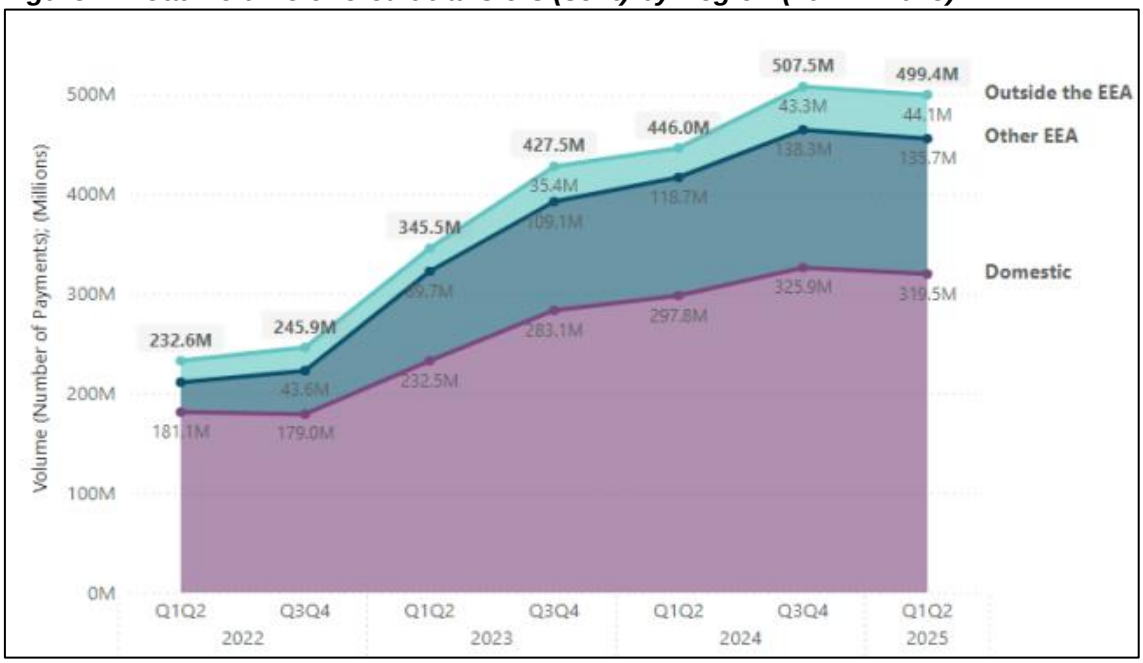
In the first half of 2025, domestic credit transfers made up 64% of total volumes. Cross-border credit transfers to countries in the EEA totalled 27%. Transfers to the rest of the world (non-EEA) accounted for 8.8% of total volumes.[184] A detailed breakdown of the total volume of credit transfers sent by region is provided in figure 7 below.

A significant proportion of cross-border transactions are processed through Retail Banks,[185] presenting ongoing challenges in detecting and reporting suspicious activity. These risks are heightened by the high volume and speed of international transfers. Criminals often exploit regulatory gaps between jurisdictions and the lack of transparency across multiple intermediaries to obscure the origin and destination of the funds. Limited information sharing between countries further hampers effective oversight, increasing the exposure of Retail Banks to ML, TF, and PF threats.

However, there have been no reported exposures of firms in the sector to jurisdictions listed on the FATF 'blacklist'.[186] Additionally in 2024, the Central Bank conducted a thematic review of the Retail Banking sector to evaluate its exposure to, and management of, ML and TF risks associated with international money flows. The review concluded that firms had established processes for identifying higher-risk jurisdictions and had implemented transaction monitoring controls to mitigate these risks. No significant concerns were identified as part of this review.[187]

[182] The Quarterly Payment Statistics published by the Central Bank are used here as a proxy for assessing transaction activity within the Irish Retail Banking sector. These statistics capture payment transactions processed by all Irish-resident payment service providers and do not exclusively reflect activity within the Retail Banking sector. Due to the absence of disaggregated data specific to Retail Banks, this proxy is the most suitable available source for indicative analysis.
[183] Payment Statistics Quarterly / 2025 / Available from: https://www.centralbank.ie/statistics/data-and-analysis/payments-services-statistics
[184] Ibid.
[185] Irish credit unions do not typically offer direct cross-border payments, as they are not authorised under PSD2. However, credit unions can support SEPA payments for euro transfers within the EU and EEA, and some may offer limited international transfers through third-party providers
[186] Financial Action Task Force / Black and Grey Lists / Available here: https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html
[187] Central Bank of Ireland data

Figure 7: Total volume of credit transfers (sent) by Region (2022 – 2025)[188]



Vulnerability 4: Cash

There has been a substantive shift away from the use of cash in recent years. For example, the number of ATM transactions declined by 46% between 2015 and 2021, whilst the use of debit cards at the point of sale increased 284% in the same period.[189] Nonetheless, cash continues to play a significant role in Ireland's financial system. In 2022, cash represented 54% of total transactions in Ireland at Point-of-Sale, and 44% of transaction value.[190] The total value of domestic cash withdrawals as of March 2025, amounted to €1 billion, and the total volume of domestic cash withdrawals for March 2025 was 7.3 million transactions.[191] At end-2024 there were just under 4,000 ATMs in Ireland, of which one-third were maintained by banks and two-thirds by independent operators.

Cash-based ML therefore remains a significant vulnerability for Retail Banks.

Traditional Retail Banks, and to a lesser extent Credit Unions, remain primary targets for criminals seeking to integrate illicit cash into the financial system. This is particularly evident

[188] Central Bank of Ireland / Payment Statistics Quarterly / 2025 / Available from: https://www.centralbank.ie/statistics/data-and-analysis/payments-services-statistics
[189] Department of Finance / Retail Banking Review / p.90
[190] European Central Bank / Study on the payment attitudes of consumers in the euro area (SPACE) – 2022 / Available from: https://www.ecb.europa.eu/stats/ecb_surveys/space/shared/pdf/ecb.spacereport202212~783ffdf46e.en.pdf / p.20
[191] Central Bank / Monthly Card Payment Statistics / 2025 / Available from: https://www.centralbank.ie/statistics/data-and-analysis/monthly-card-payment-statistics

in cash-based ML typologies, where the physical deposit of illicit funds is facilitated through financial institutions with high cash-handling volumes. Despite the overall decline in cash usage, law enforcement intelligence consistently underscores that cash continues to be the medium of choice for a broad spectrum of criminal enterprises, including drug trafficking, smuggling, human exploitation, and tax evasion.

Unlike traditional Retail Banks, digital-only banks operating in Ireland do not maintain physical branches or offer extensive cash-handling infrastructure. However, some cash handling services are available via Point of Sale at retail outlets, and third-party involvement may lead to further complexities and vulnerabilities. Given the limited, they are not directly exposed to the same extent as Traditional Retail Banks to the placement stage of cash-based ML. However, these institutions may still be exploited after the placement of illicit cash within the financial system.

Vulnerability 5: Implementation of Instant Payments

The rise of instant payments, driven by EU initiatives,[192] has increased vulnerabilities related to ML, TF, and PF, as they enable illicit funds to be moved more swiftly between accounts and across borders, and inhibit Retail Banks' ability to conduct real-time monitoring. This has required Retail Banks to adapt control environments to the risks posed. To mitigate these risks and typologies, Irish Retail Banks are adopting new 'RegTech' solutions, including adoption of AI and machine learning to better identify potentially suspicious transaction flows.

[192] European Parliament and Council of the European Union / Regulation (EU) 2024/886 of the European Parliament and of the Council of 13 March 2024 amending Regulations (EU) No 260/2012 and (EU) 2021/1230 and Directives 98/26/EC and (EU) 2015/2366 as regards instant credit transfers in euro / Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202400886

Case Study: International PPSN and Account Fraud – Organised Cybercrime Group

This case involved a sophisticated fraud scheme exploiting Irish PPSNs ("PPSN", a unique reference number that helps Irish residents access social welfare benefits, public services and information) and accounts, orchestrated by an organised cybercrime group with international connections.

The group compromised PPSNs and personal details of 26 employees at an Irish nursing home to fraudulently claim Pandemic Unemployment Payments, obtaining approximately €49,500 from the Department of Social Protection. The use of false PPSNs and identity documents was central to the scheme. Additionally, the investigation uncovered BEC fraud targeting companies and Credit Unions, where salary payments were redirected to Irish bank accounts controlled by the group and subsequently transferred to international accounts.

Fraudsters set up and used a mix of genuine and false accounts, including their own accounts, accounts opened under false identities, and accounts belonging to recruited money mules. In total, 21 accounts were used, with 14 directly linked to the accused (six genuine, eight false). Accounts were opened at traditional banks, with false documentation such as Dutch ID cards and UK driving licences used to falsify the KYC controls during account creation.

The scheme utilised a range of financial institutions, including Irish banks, EMIs, and international banks, including in Germany. The operation had clear international links, with fraudulent documents sourced from criminals in Amsterdam, and funds transferred to accounts in the UK and Germany. Communications also indicated connections to Ghana for further account preparation and laundering activities.

Consequence

Retail Banking is central to the effective functioning of the Irish economy. A substantive ML, TF or PF incident in the sector would be damaging both in terms of the impact of the event and its effect on customers and the wider public, as well as the fact that it would be highly likely to cause significant damage to Ireland's international reputation. As such, the consequence has been rated as very significant.

EU Supranational Risk Assessment

The EU Supranational Risk Assessment assessed the Retail Banking sector in its most recent (2022) risk assessment as detailed below:

TF Risk	ML Risk
Significant	Very Significant

The risk factors identified within this sectoral risk assessment are aligned with those set out in the EU Supranational Risk Assessment.

Horizon Scanning

Artificial Intelligence and Machine Learning

AI and machine learning technologies are increasingly being explored within the Irish Retail Banking sector to enhance fraud detection, strengthen AML controls, and improve the efficiency of risk management operations. These technologies offer the ability to process and analyse vast volumes of transactional data in real-time, enabling the identification of anomalous patterns and potentially suspicious activities with greater speed and accuracy than traditional rule-based systems. Discussions with stakeholders in the Retail Banking sector indicate a clear strategic shift toward integrating AI and machine learning into control frameworks. However, full-scale implementation remains in progress, with many institutions still in the early or pilot stages of adoption. These technologies also present a ML, TF, and PF risk: just as financial institutions are leveraging AI and machine learning to strengthen defences, criminals are adopting them to develop more sophisticated and scalable operations, including advanced phishing schemes, synthetic identity fraud, and automated social engineering attacks. This evolving threat landscape underscores the need for continuous innovation and vigilance in the deployment of AI-driven financial crime controls.

Virtual IBANs

In the EU AML Regulation, a Virtual International Bank Account Number (‘‘vIBAN’’) is defined as ‘an identifier causing payments to be redirected to a payment account identified by an IBAN different from that identifier’. As the European Banking Authority (‘‘EBA’’) has noted, while the use of vIBANs provides benefits for recipients of funds transfers, they also create novel ML/TF risk. This is mainly because the end user of a vIBAN may be effectively unknown to the payment service provider. This creates challenges around CDD effectiveness, transaction monitoring, and reporting of suspicious transactions.

Non-Retail Banking

Executive Summary

	2019 Risk Ratings	2026 Risk Ratings
Higher Risk Business Activities		
ML	Not Assessed	Significant
TF	Not Assessed	Significant
PF	Not Assessed	Low
Asset Finance		
ML	Not Assessed	Low
TF	Not Assessed	Low
PF	Not Assessed	Low
Securities Transactions		
ML	Not Assessed	Moderate
TF	Not Assessed	Low
PF	Not Assessed	Low
Depositary Services		
ML	Not Assessed	Moderate
TF	Not Assessed	Low
PF	Not Assessed	Low
Covered Banks		
ML	Not Assessed	Low
TF	Not Assessed	Low
PF	Not Assessed	Low

**There were no sub-sector ratings in the 2019 NRA; the Non-Retail Banking sector overall was assessed as Medium-High for ML/TF.*

Key Insights

Firms classified as undertaking higher-risk business activities have been rated significant for both ML and TF. This is due to the complexity of transactional activity and heightened exposures to cross-border activity, including some exposure to high-risk jurisdictions with weak AML/CFT regimes. The type of NRB customers can often heighten risk due to the scale and scope of their activities.

The other sub-sectors have been assessed as low and moderate for ML, and low for TF, due to the inherently low risk of the activities. The lower rating for PF reflects the generally limited exposure of these activities to jurisdictions associated with PF concerns.

The key vulnerabilities in the sector are:

- **Geographic and cross-border exposure:** NRBs in Ireland are internationally focused, which creates vulnerabilities particularly where customers or transactions involve jurisdictions with lower regulatory standards. However, direct exposure to high-risk jurisdictions is limited.

- **Complex products, services and high-value transactions:** NRB products and services often involve complexity, high value and volume, creating risks particularly through indirect exposure such as correspondent banking and the offering of NRB services to PI and EMI customers, which require strong controls.

- **Outsourcing:** Use of third-party or group entities for certain functions is increasingly common among NRB firms, which can pose risks if not properly managed.

- **Nature of the customer base:** The prevalence of high-net-worth individuals ("HNWIs") and complex structures in the NRB customer base increases complexity and vulnerability. The sector also has exposure to 'retail' customer bases, including through correspondent banking and the offering of NRB services to PI and EMI clients. Exposure to PEPs is also present and is higher than in Retail Banking, although lower than for investment firms.

Defining the NRB Sector

NRBs can be broadly categorised by their dominant activity. These are:

1. **NRBs with higher-risk activities:** Such credit institutions are typically branches[193] or subsidiaries of global entities. The services offered are varied and can include corporate banking and corporate finance services, private banking, corporate trust services, treasury services, trade finance and correspondent relationships. These banks primarily operate on an international basis, serving customers and counterparties globally, and processing significant volumes and values of international transactional activity.

2. **NRBs specialising in asset finance:** Credit institutions that provide short-term finance to a customer for the purchase of a product or service from them, or from an affiliate firm. This activity is inherently lower risk as they are used for specific, time-bound

[193] Branches established under the freedom of establishment basis or third country branches

business purposes and are typically offered to known clients with established relationships, reducing anonymity and opportunities for misuse.

3. **NRBs specialising in securities transactions:** Credit institutions that facilitate their customers in the purchase, selling or management of securities such as bonds, mortgage-backed securities, or money market products. These institutions typically have low customer numbers and most report that activities are limited to the EEA.

4. **NRBs specialising in depositary services:**[194] Credit institutions that offer custodian and fiduciary services to their customers, who are predominately fund vehicles. Given the nature of the customer base, depository services have a significant international focus. This activity is inherently lower risk.

5. **Covered banks:** These are generally subsidiaries of larger banking groups set up to hold assets and present low risk given the type of activity involved.

Scale and Structure of the NRB Sector in Ireland

Ireland has long been an attractive location for multinational corporations to base their European operations. Growth in the presence of non-Irish NRBs began in earnest in the 1990s, with a change in the landscape after 2016 as firms moved activity to Ireland due to the impact of the UK's departure from the EU. NRBs can deal with customers across the EEA under the freedom of service[195] and freedom of establishment[196] provisions.

Ireland's NRB sector is moderately outsized, in line with the country's banking assets and financial sector employment which are both somewhat higher than the EU average. There has been a small decline in the population of NRBs in recent years, mainly of banks conducting lower-risk activities. However, the sector continues to have a large presence, with 40 NRBs operating in Ireland[197] in June 2025, almost all of them being subsidiaries or branches of global financial institutions with parents in the UK, EEA or North America, and

[194] Central Bank of Ireland / Authorised Firms Providing Depositary Services as of 31 March 2025 / There were 21 Firms authorised by the Central Bank with a primary business activity of providing depositary services. Of these 21, 10 hold banking licenses. Typically, these firms are entities that have been issued banking licenses in order to hold fund's securities for safe keeping. They are typically part of large and reputable financial groups and because they hold banking licenses, they may be authorised to provide additional banking services. The remaining 11 firms, fall with the Fund Service Provider (FSP) population and are generally subsidiaries of large FSP groups. However, depositaries within the FSP population are not authorised to provide additional services

[195] Credit Institutions legally operating in one member state may offer and provide services in other member states on a temporary basis while remaining in their country of origin.

[196] Credit Institutions legally operating in one Member State may carry out an economic activity in a stable and continuous way in another Member State

[197] Central Bank of Ireland data

with total assets reported by firms in the Central Bank's regulated population at €485 billion in 2024.[198] In 2024,[199] the total customer base for NRBs reached 2.1 million, comprising both private and corporate customers in Ireland and internationally.

The NRB sector is predominantly focused on international business, although those NRBs which focus on asset finance and covered banks are more domestic in nature. A large majority (79%) of NRBs do not restrict their activities to the EEA, 13% are EEA only, and just 8% are domestic only.[200] Some NRBs established outside Ireland also passport in their services to Ireland on an FOS basis, however these are not designated entities in Ireland and have not been considered in this assessment.

Threats and Vulnerabilities

Threats

The overarching ML, TF, and PF threats experienced by Ireland are set out above. The NRB sector faces heightened exposure to several key threats including fraud, cybercrime, and sanctions evasion, largely due to the complexity of its customer base, the high value and volume of transactions and the cross-border nature of activities. Fraud schemes often exploit complex corporate structures and HNWIs, while cyber threats target increasingly digitalised operations.

Sanctions evasion remains a significant concern, with illicit actors using complex transaction layering across jurisdictions with weaker controls and jurisdictions where EU, US, UK and other sanctions obligations do not apply. This threat is heightened by the NRB sector's international exposure, correspondent relationships, and payment firms as clients, which expose the sector not only to direct risks but also to the activities and risks associated with these firms' underlying clients.

In 2024, a total of 1,444 STRs were submitted by NRBs. Approximately 59% of analysed STRs were disseminated; ≈3% to law enforcement within Ireland for further investigation and ≈56% disseminated to other FIUs for their information. Of the total STRs submitted in 2024 approximately 95% cited ML as the basis for submission.

[198] Central Bank of Ireland data
[199] Central Bank of Ireland data
[200] Central Bank of Ireland data

Vulnerabilities

Vulnerability 1: Geographic and Cross-Border Exposure

Many NRB product offerings are inherently cross-border in nature. Cross-border activity creates vulnerabilities, particularly when it involves customers and transactions in jurisdictions with lower regulatory or supervisory standards, or where there are heightened financial crime risks associated with the jurisdictions. However, based on information in regulatory returns, Ireland has very limited exposure to countries listed on the FATF blacklist or grey list.[201]

The international response to the Russian invasion of Ukraine – including the imposition of trade and financial sanctions – has required some firms in the NRB sector to enhance their control frameworks to respond to the increased inherent sanctions risk, and the additional complexity which has been created in the sanctions landscape.

Vulnerability 2: Complex Products, Services and High-Value Transactions

Many products and services offered by the NRB sector have the characteristics of speed, high volumes and values of transactions. In some instances, products and services offered by NRBs to their customers present additional risk via the underlying customers of the NRB customers, for example, correspondent banking services or services provided to PIs. NRBs' systems and controls need to be commensurately sophisticated to mitigate such risks. However, it is noted the prevalence of such services is not widespread in the NRB sector in Ireland, albeit some individual NRBs are heavily exposed and report the provision of such services as a key risk area.

Vulnerability 3: Outsourcing

As many of the firms in the sector are part of wider global groups, NRBs often outsource aspects of their operations – including their AML/CFT functions – to intra-group or external providers. While outsourcing can offer significant benefits, such as access to specialist resources and technology, it necessitates robust oversight by the Irish-regulated firm to ensure effective delivery of outsourced processes. Where not adequately controlled or overseen, outsourcing can contribute to weakened AML/CFT/CPF and sanctions controls.

[201] Financial Action Task Force / Black and Grey Lists

Around 80%[202] of NRBs outsource some aspect of their systems and controls, a number which has remained stable in recent years.

Case Study: Failure to implement effective transaction monitoring controls

In 2022, an EU bank operating in Ireland under passporting rules was fined €1.8 million by the Central Bank of Ireland for historical failures in its transaction monitoring. The Irish branch excluded certain customer categories from monitoring, including some rated high-risk, due to system misconfigurations. The Central Bank found the bank had not properly tailored its monitoring system to meet CJA requirements, and that the Irish branch was unaware that its customers had been excluded from monitoring for four years, despite this being flagged in an internal audit.

This case highlights the requirement for obliged entities to ensure that systems, controls, policies and procedures, delivered either by intra-group or by external providers, are compatible with Irish legal requirements and that their governance framework and risk management measures operate effectively.

Vulnerability 4: Nature of the Customer Base

NRBs generally have customer types with greater complexity such as corporate customers and HNWIs. The intricacy of NRBs' customers' affairs - characterised by activity in multiple jurisdictions, opaque ownership structures lending complexity to identifying beneficial ownership, and large transactions - presents heightened ML/TF risks. Regarding PEPs, the NRB sector in Ireland reported more PEP exposure than Retail Banks, although the share is lower than for investment firms. In addition, feedback from engagement with sector participants indicates that onboarding PI/EMI firms presents challenges, especially due to difficulties in identifying and understanding the underlying customer base of these firms. This adds complexity to the due diligence process and increases the risk profile of the sector. As noted in the PI/EMI sectoral risk assessment, many firms within the sector have a strong technology and growth focus but a less developed compliance culture, highlighting the need for control frameworks.

[202] Central Bank of Ireland data

Consequence

Ireland's NRB sector is moderately outsized compared to the average for other EU countries, and hosts the EU headquarters of some large global banks and other NRBs with a cross-border focus. As a result, there are substantial flows of funds and assets through Irish NRBs. A material ML, TF or PF incident in this sector would adversely affect national interests and the reputation of the financial sector. As such, the consequence has been rated as significant.

EU Supranational Risk Assessment

The EU Supranational Risk Assessment assessed the Corporate Banking and Private Banking sectors in its most recent (2022) risk assessment as per the below:

Sub-Sector	TF Risk	ML Risk
Corporate Banking	Lowly Significant	Significant
Private Banking	Not Relevant	Significant

The risk factors identified within this sectoral risk assessment are aligned with those set out in the EU Supranational Risk Assessment.

Horizon Scanning

Sanctions and Geopolitical Risks

Irish NRBs, due to their international focus, are exposed to sanctions risks. Since the Russian invasion of Ukraine, financial sanctions obligations have heightened the need for robust sanctions control frameworks. These frameworks require a combination of customer and transaction screening, along with stronger links to due diligence processes. There have been considerable efforts to reduce exposure to high-risk jurisdictions and entities by Irish firms, including in the NRB sector. Eurostat data suggests that Russian financial assets held by Irish-resident firms and households fell from nearly €12 billion at the end of 2021 to €171 million by the end of 2024.[203]

[203] Eurostat / International Investment Position - Quarterly and Annual Data (BPM6), Financial Account: Portfolio Investment

Funds

Executive Summary

	2019 Risk Ratings	2026 Risk Ratings
Investment Funds		
ML	Medium-High	Significant
TF	Medium-High	Moderate
PF	Not Assessed	Low
Funds Management Companies		
ML	Medium-Low	Significant
TF	Medium-Low	Moderate
PF	Not Assessed	Low
Funds Administrators		
ML	Medium-High	Significant
TF	Medium-High	Moderate
PF	Not Assessed	Low
Funds Depositories		
ML	Medium-High	Significant
TF	Medium-High	Moderate
PF	Not Assessed	Low

Key Insights

Ireland is a leading global hub for investment funds; the sector has expanded materially, marked by sustained growth in Assets Under Management ("AUM"), revenue, and employment. The sector's structure and operations also present vulnerabilities that can be exploited for ML, TF, and PF.

The key vulnerabilities in the sector are:

- **Opacity of investor identity and ultimate beneficial ownership:** Complex investment, legal and/or ownership structures used to invest in funds can result in challenges to establishing the identity of the ultimate beneficial owner of the investor. For example, the use of nominee accounts by financial intermediaries such as brokers and investment advisors can be exploited to integrate illicit proceeds into the financial system.

- **Cross-Border Financial Flows:** The global nature of the funds sector facilitates the cross-border movement of large amounts of funds to facilitate the purchase of assets which could potentially attract bad actors seeking to move large volumes of illicit funds. However, funds are subject to reporting and customer due diligence obligations when

implementing their investment strategies. This includes depositary oversight and audits of their cashflows that mitigate against the use of an investment fund to conduct such activity.

- **Use of Intermediaries and Third Parties:** Investment funds typically delegate the operational elements of functions such as investment management, fund administration and distribution to other entities. In general, these delegates are themselves regulated entities subject to regulatory requirements and the fund management company ("FMC") retains responsibility for ensuring the delegated function is conducted in accordance with the relevant regulatory requirements. Funds may also invest through intermediary investment vehicles, including special purpose vehicles ("SPVs") and co-investment structures, which can increase the complexity of the overall structure. The use of such arrangements can potentially weaken oversight of ML, TF, and PF risks.

- **Broad and Diverse Investor/Customer Base:** The diverse investor base (PEPs, high-risk jurisdictions, HNWIs, complex structures) can heighten ML, TF, and PF risk; exposure is largely indirect, however as distribution is generally mediated through intermediaries that are obliged entities with their own AML/CFT obligations.

Overall, the PF risk for the funds sector is assessed as low given limited direct exposure to high-risk jurisdictions, the nature of fund products, and the regulatory requirements imposed on authorised investment funds.

Legislative and Regulatory Framework for the Funds Sector

Regarding AML/CFT, authorised Undertakings for Collective Investment in Transferable Securities ("UCITS"), Alternative Investment Fund ("AIF"), FMCs, funds administrators, and other relevant entities providing fund services in Ireland are considered 'designated persons' under the CJA and are supervised by the Central Bank. Authorised investment funds are also subject to specific obligations and requirements set down in the UCITS and AIF Managers Directives as transposed into Irish law which are further supplemented by the Central Bank's UCITS Regulations and AIF Rulebook.

Scale and Structure of the Funds Sector in Ireland

Ireland is a global hub for funds and is the third largest global centre and the second largest in Europe. Industry sources suggest that Ireland has a total of 997 fund promoters from 50 countries which have selected Ireland as the domicile and/or servicing location for their

funds.[204] The net asset value ("NAV") of Irish-resident investment funds measured €5.309 trillion in the third quarter of 2025. It has increased four-fold since the first quarter of 2014 through a combination of net transactions and increases in valuations.[205]

As of October 2025, the Central Bank has registered a total of 10,284 investment funds including sub-funds, 142 Fund Management Companies, and 42 funds administrators.[206]

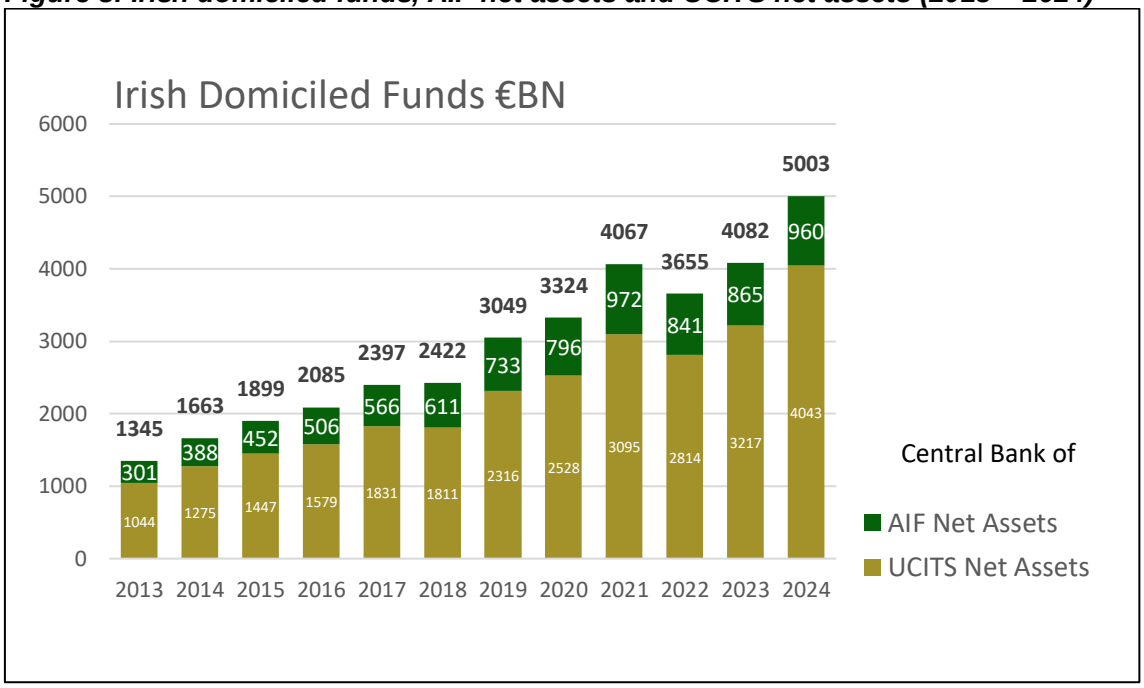
Investment Funds

Investment funds are established for the purpose of investing the pooled funds of investors (held as units or shares) in assets in accordance with investment objectives and investment policies published in a prospectus. Assets of the fund are managed by FMCs and are held for safekeeping by an independent depositary. The depositary is also responsible for monitoring fund cashflows, monitoring compliance with fund rules and regulatory requirements, and ensuring that the interests of the fund's investors are safeguarded. Where a fund makes investments through intermediary investment vehicles, the depositary also has a look-through obligation where those vehicles are controlled by the fund. While an investment fund is a legal entity and a designated person under the CJA, most of its operations and activities are conducted under contractual arrangements by a variety of FSPs including an FMC ("ManCo"), funds administrator and depositary.[207]

In Ireland, investment funds are authorised as UCITS and AIFs, each operating under distinct regulatory frameworks and subject to authorisation and supervision by the Central Bank. UCITS and AIFs can be structured as unit trusts, variable or fixed capital investment companies, Investment Limited Partnerships and ICAVs. Additionally, Common Contractual Funds ("CCFs") can be used as a structure for both UCITS and certain AIFs.[208]

[204] Irish Funds / Why Ireland 2025 / Available from: https://cdn.irishfunds.ie/x/3cff3aa561/7473-irish-funds-why-ireland-2025-euro-_web.pdf / p.5
[205] Central Bank of Ireland, Investment Fund Statistics, Q3 2025 / Available from: https://www.centralbank.ie/docs/default-source/statistics/data-and-analysis/other-financial-sector-statistics/investment-funds/2025q3---information-release-investment-fund-statistics.pdf?sfvrsn=49446c1a_6
[206] Central Bank of Ireland data
[207] Central Bank of Ireland data
[208] Ireland offers a diverse range of fund structures, each governed by a comprehensive legal and regulatory framework. For further details on the primary fund structures available in Ireland, please refer to the Legal Persons and Arrangements section of this assessment.

Figure 8: Irish domiciled funds, AIF net assets and UCITS net assets (2013 – 2024)[209]



Fund Management Company ("FMC")

Investment funds must appoint an FMC to manage the fund and oversee its overall governance and compliance with regulatory requirements. The FMC is responsible for appointing the depositary, the day-to-day running of the fund including investment decisions, fund administration, risk management, compliance and delegated oversight. These functions ensure that the fund is financially sound, risks are properly managed, investment activities are monitored, and all regulatory obligations are met.

In addition to these core responsibilities, the FMC must maintain effective oversight of any delegated functions, such as administration or investment management, ensuring they are carried out to the required standard. It is also expected to uphold strong governance frameworks, board reporting, and internal controls. The regulatory framework also sets out specific requirements to ensure that the FMC is not a letterbox entity, and the FMC must demonstrate sufficient local presence, expertise, and operational substance, avoiding the risk of being classified as a letterbox entity.[210]

[209] Irish Funds / Why Ireland 2024 / p.3
[210] A "letterbox entity" refers to an FMC that has delegated so many of its functions to third parties (e.g., investment managers, administrators) that it no longer retains meaningful control or oversight of the fund's operations.

Funds Administrator

Funds administrators are responsible for maintaining the fund's books and records, including NAV calculations, valuations, financial reporting and investor services. The funds administrator is also responsible for the onboarding and completion of CDD and other AML/CFT/CPF controls, processing subscriptions and redemptions, issuing confirmations, and handling investor reporting.

Fund Depositary

Authorised investment funds are required to appoint an independent depositary which is responsible for the custody and safekeeping of the fund's assets. The depositary also monitors the fund's cashflows and activities to ensure compliance with both the fund rules and its regulatory obligations. The depositary plays a critical role in safeguarding the interests of the fund's investors and has specific reporting obligations to the Central Bank where it identifies potential issues of concern.

The risks associated with depositaries have been considered within the Non-Retail Banking sectoral risk assessment (see section Non-Retail Banking sectoral risk assessment). Although not all Fund Depositaries are banks, the associated risks are broadly similar.

Threats and Vulnerabilities

Threats

The overarching ML, TF, and PF threats experienced by Ireland are set out above. Similar to other financial sectors, the funds sector faces exposure to threats including the use of criminal proceeds to purchase fund-related products, the concealment of beneficial ownership, and the use of investment activity to justify criminal proceeds such as profit obtained from other illicit activity.

The funds sector is also exposed to investment fraud as a predicate offence and market abuse (which comprises insider dealing, market manipulation, and unlawful disclosure of inside information, albeit such offences are covered by the EU Market Abuse Regulation and the EU Criminal Sanctions for Market Abuse Directive).

In theory, funds could be misused or diverted to finance terrorist organisations. Evidence to date indicates minimal use of the funds sector for terrorist financing globally and none

identified in Ireland, so the sector is assessed as an unlikely vehicle for TF in the Irish context.[211]

A total of 480 (183 STRs[212] and 297 STReu[213]) STRs were submitted by firms in this sector in 2024. Of those that have been fully analysed, ≈17% were disseminated; ≈1% to law enforcement within Ireland and ≈16% to other FIUs. 95% of the STRs submitted cited ML as an indicator.

Vulnerabilities

Vulnerability 1: Opacity of Fund Structures and Beneficial Ownership

The funds sector in Ireland uses a variety of legal structures for funds and for investor investments. While fund structures are set by legislation and do not of themselves obscure beneficial ownership, investor investment channels may involve complex entities that can obscure ownership. However, these entities are subject to AML/CFT obligations and, where controlled by the fund, depositary look-through obligations apply.

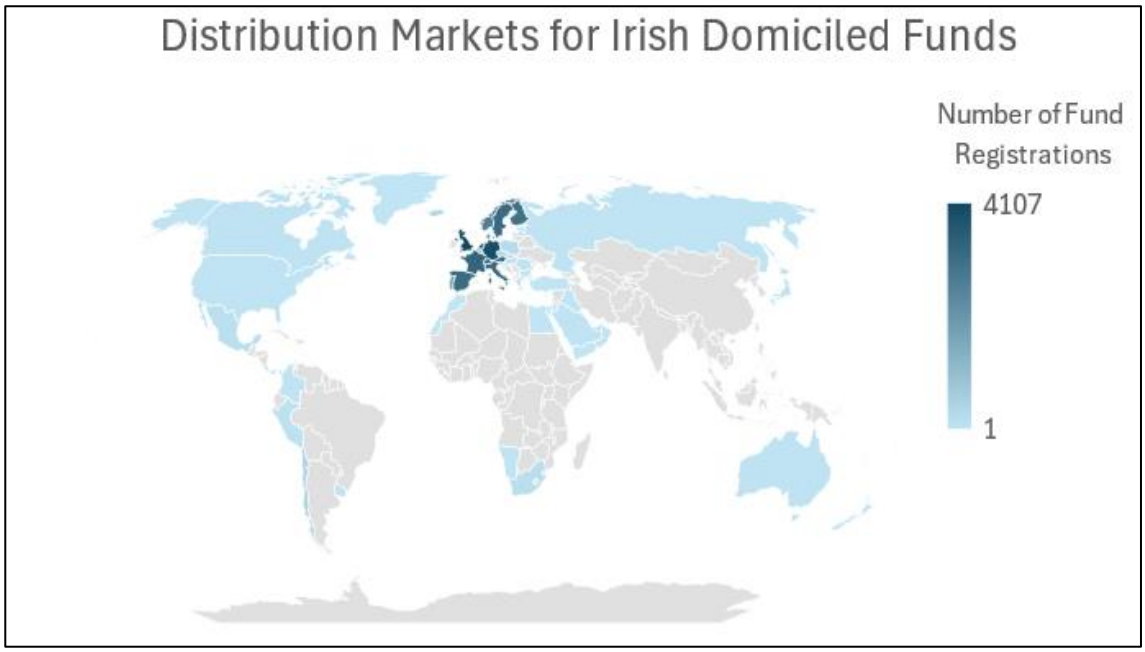
Vulnerability 2: Cross-Border Financial Flows

The funds industry operates internationally, through fund domicile, marketing, and investment locations, facilitating large cross-border asset movements, including to higher-risk or low-transparency jurisdictions. However, funds remain subject to strict transparency, reporting, and regulatory oversight obligations regardless of ownership structures.

Ireland serves as a leading domicile for investment funds, with a broad range of Irish-domiciled funds distributed globally through a network of international distributors. Central Bank regulatory returns data shows that a small minority of firms have operations and activities and customer base exclusively in Ireland. For most firms, the majority of business activity is international, with business conducted either elsewhere in the EU or on a global basis.

[211] Department of Justice / Ireland Terrorist Financing Risk Assessment / p.17
[212] Designation is selected by the entity at registration.
[213] STReu is a specific report, usually submitted by entities located in Ireland and passporting their services to other EU countries, where there is no nexus to Ireland. All 297 of these reports have been processed and disseminated to the relevant EU FIU.

Figure 9: Number of Irish domiciled funds registered for distribution



Jurisdictions of Heightened Risk

The table below highlights the distribution of Irish funds across jurisdictions that have an overall Basel AML Index score above 5.5, suggesting a heightened risk of ML, TF or PF. It also specifies whether these jurisdictions are listed on the FATF grey list[214] or designated as high-risk third countries by the EU[215] as of December 2025.

[214] Financial Action Task Force / Black and Grey Lists
[215] Commission Delegated Regulation (EU) 2025/1184 of 10 June 2025 amending Delegated Regulation (EU) 2016/1675 (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02025R1184-20250910) Accessed 31/12/25

Table 19: Distribution of Irish funds by jurisdiction with Basel AML Index scores above 5.5[216]

Distribution Jurisdictions	Irish Domiciled Funds Registered for Distribution	Basel Overall Risk Score	FATF Grey List	EU High-risk third countries
South Africa	145	5.7	N	Y
United Arab Emirates	96	6.2	N	N
Gibraltar	49	Not scored	N	N
Saudi Arabia	16	5.9	N	N
Kuwait	1	6.3	N	N
Panama	1	5.9	N	N
Lebanon	1	5.8	Y	Y
Türkiye	1	5.6	N	N
Yemen	1	Not scored	Y	Y

While Irish-domiciled funds operate globally and may interact with higher-risk jurisdictions, the actual exposure is limited: only 0.6% of global distributions are to high-risk locations, and none to PF-sanctioned countries. There remains potential for indirect exposure via links or sanctions circumvention, but overall ML, TF, and PF risks are assessed as low and are managed within a robust regulatory framework.

The top five distribution markets for Irish-domiciled funds account for 35% of all global distribution activity involving these funds. These leading markets are either EU member states or jurisdictions with well-developed regulatory frameworks.

Table 20: Overview of AML/CFT/CPF risk levels across key fund distribution markets

Distribution Jurisdiction	Irish Domiciled Funds Registered for Distribution	Basel Overall Risk Score	Basel Country Ranking
United Kingdom	4,107	4.1	140
Germany	3,922	4.6	114
Switzerland	3,355	4.5	124
France	3,290	3.9	151
Netherlands	3,214	4.5	120

[216] PwC Luxembourg / Global Fund Distribution 2024 / Available from: https://www.pwc.lu/en/fund-distribution/docs/pwc-publ-gfd-2024.pdf

Vulnerability 3: Use of Intermediaries and Third Parties

Regulated intermediaries and third parties play a key role in fund distribution, management, administration, and investment activities. However, the funds framework includes specific safeguards to address risks related to oversight, transparency, and investor identification, ensuring that these structures are designed for transparency and regulatory access—not to obfuscate investors or investments. It also requires institutions to rely on the adequacy of AML/CFT/CPF controls implemented by other entities, which can be particularly concerning when those entities operate in jurisdictions with different or less stringent regulatory frameworks or weaker enforcement.

The Central Bank addressed these issues in its Anti-Money Laundering Bulletin published in November 2021 where it highlighted weaknesses in AML/CFT control frameworks caused by a lack of oversight of outsourcing arrangements to third parties within the funds sector. This, along with overall adequacy of AML/CFT systems and controls, continues to be a focus of supervisory activity for the Central Bank.

These vulnerabilities collectively underscore the importance of robust, end-to-end AML/CFT/CPF frameworks and effective oversight across all intermediary functions in the funds sector.

Vulnerability 4: Complexity of Transactional Activity

The complexity of some funds' trading could, in the abstract, be used to layer illicit funds, but this is mitigated to some extent by the control framework in place. Transactions typically flow through regulated intermediaries (banks, depositaries) and are monitored by automated systems and regulatory oversight, reducing practical exploitability.

Vulnerability 5: Broad and Diverse Investor/Customer Base

The broad and diverse investor base within the funds sector adds another layer of complexity to AML/CFT efforts. The investor base includes high-risk customer types, such as PEPs, customers with links to high-risk countries or HNWIs, and complex corporate structures, all of which create risks inherent in the sector, and which heighten exposure to ML, TF, and PF.

Consequence

Ireland's funds sector is a significant industry, and as noted has significant domestic and international exposure. A substantive ML, TF or PF incident in the sector would cause significant harm related to the underlying offences, as well as to the integrity of the

international financial markets and Ireland's reputation, with potential long-term implications. As such, the consequence has been rated as very significant.

EU Supranational Risk Assessment

While the funds sector was not specifically assessed as a standalone category in the SNRA, it was partially covered within the broader Retail and Institutional Investments Sector. As such, relevant findings and vulnerabilities outlined in the SNRA can be considered applicable, at least in part, to Ireland's funds sector.

The EU SNRA assessed the Retail and Institutional Investments Sector in its most recent (2022) risk assessment as per the below:

TF Risk	ML Risk
Non-Relevant	Significant

Horizon Scanning

The following are new and emerging threats and vulnerabilities which may have an impact on the funds sector.

Sector Growth and Market Trends

A notable area of growth in the funds sector is that of private asset investments. They are generally considered to be non-publicly traded assets, including inter alia, private equity, venture capital, private credit, real estate and infrastructure. The growth in demand for private asset investments may increase the risk and potential vulnerabilities to illicit financial flows. Potential vulnerabilities include increased complexity in the investment process and more opaque or complex legal and ownership structures which are commonly used to facilitate investments in private asset strategies.

Crypto-assets

Executive Summary

	2019 Risk Ratings	2026 Risk Ratings
ML	Medium-High	Very Significant
TF	Medium-High	Very Significant
PF	Not Assessed	Low

Key Insights

The use of crypto-assets has significantly increased and become more mainstream over the last ten years. Crypto-assets were originally designed to be a payment instrument; however, their primary use to date has been for speculative investment purposes, rather than for third-party payments. However, where crypto-assets are used for third-party payments, the ML, TF, and PF risk is significantly heightened; this can be seen with the use of crypto-assets as a payment mechanism in ransomware payments, drug trafficking, and other illicit activities. The recognition of the primary use of crypto-assets for speculative investment purposes is reflected in the legislative framework for crypto-assets, which mirrors that used to regulate investment services and markets. However, what sets this sector apart from investment services and markets is the ease of use of crypto-assets for third-party payments.

The key vulnerabilities in the sector are:

- **Anonymity or Pseudonymity:** Crypto-asset products can conceal identities, which complicates transaction tracing and the detection of illicit activities, especially where there are decentralised networks and/or privacy-enhancing technologies (“PETs”), which can limit transparency of funds before they reach regulated CASPs, making illicit activity harder to detect.

- **Inconsistent international regulation:** Gaps in global AML/CFT rules, including weak Travel Rule enforcement, expose Irish-regulated CASPs to risks in cross-border transactions. The implementation of MiCAR will help to harmonise regulations across the EU, mitigating these risks.

- **Speed and cross-border transaction risk:** Rapid settlement can be exploited, particularly when combined with the ability to transfer assets across borders, challenging authorities to detect and intervene in real-time and/or to track assets internationally.

- **Complexity and rapid evolution of products and services:** The rapid development and increasing complexity of crypto-asset products, such as cryptocurrencies, Decentralised Finance ("DeFi") platforms, mixers and atomic swaps create diverse risk profiles. Irish-regulated CASPs must continually update risk assessments and compliance frameworks to address these complexities.

- **Resourcing, outsourcing, and intelligence gaps:** Irish-regulated CASPs face challenges in hiring risk and compliance staff with both expertise in the underlying technology and knowledge of the AML/CFT requirements. Additionally, regulated CASPs who outsource key risk management functions to group entities, can create gaps in the effectiveness of their AML/CFT frameworks, especially when the group entity has not appropriately tailored its service to the local Irish context. The absence of widespread information sharing frameworks between CASPs and traditional financial institutions also limits the sector's ability to detect ML/TF/PF patterns and mitigate risks.

- **Unregulated area of Crypto-assets:** Unregulated areas within the crypto-assets sector – including in Ireland – pose risks to the financial system, including DeFi and P2P transactions.

Legislative and Regulatory Framework for the Crypto-assets Sector

Markets in Crypto-assets Regulation ("MiCAR")

The EU brought into force MiCAR in June 2023[217] which introduced a new regulatory framework for crypto-assets, bringing more of the sector under the regulatory umbrella. MiCAR became applicable to issuers of asset-referenced tokens and e-money tokens on 30 June 2024 and applicable to CASPs on 30 December 2024, and establishes a harmonised, European-wide regulatory framework that applies uniformly across all member states. This replaces the prior national framework for VASPs which was governed by national legislation, and only required them to comply with AML and CFT obligations and to register with the Central Bank for AML/CFT purposes.[218]

[218] The European Union's Fifth Anti-Money Laundering Directive ('5AMLD') was transposed into Irish law (23 April 2021) by way of the Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2021.

After a one-year transition period, the previous Irish regulatory regime for VASPs ceased to apply from 30 December 2025 at which point it was replaced by the CASP authorisation regime. All registered VASPs that intended to continue to operate following the 12-month transitional period, i.e. post 30 December 2025, required a CASP authorisation from the Central Bank or from another EU member state competent authority. At end-December 2024 there were 22 licensed VASPs in Ireland, but due mainly to authorisation in other EU member states, there are just 3 CASPs licensed as of January 2026.

The CASP authorisation regime introduced under MiCAR is significantly broader than the previous VASP framework, including expanding the scope beyond AML considerations to include prudential and consumer protection requirements. Under MiCAR, a broader range of activities/services will now be subject to its regulatory requirements, expanding the scope of oversight and ensuring that more entities within the financial sector adhere to the new framework.

Transfer of Funds (Recast) Regulation

The Transfer of Funds (Recast) Regulation[219] published in June 2023, extended the obligation to include information about the originator and beneficiary of crypto-asset transfers. The EBA has also issued corresponding guidance,[220] which became applicable as of 30 December 2024 and provides details on how certain provisions of the Recast FTR should be complied with by CASPs. The changes introduced by the Recast FTR are wider than the obligation to include information on crypto-asset transfers. In addition to this obligation, Article 23 of the Recast FTR imposes an obligation on payment service providers and CASPs to have policies and procedures to ensure the implementation of EU Financial Sanctions.

Scale and Structure of the Crypto-asset and Crypto-asset Service Provider Sector in Ireland

In recent years, the rapid growth and adoption of crypto-assets, such as cryptocurrencies, tokens, and other digital financial instruments, have raised significant regulatory and supervisory challenges across the globe, including in Ireland. This emerging regulatory framework underscores the sector's growing significance, as it attracts both institutional and retail investors, as well as becoming more widely adopted in the global economy. Although

[219] Regulation (EU) 2023/1113
[220] European Banking Authority / Guidelines on Information Requirements for Transfers of Funds and Crypto-Assets / 2024 / Available from: https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/anti-money-laundering-and-countering-financing-terrorism/guidelines-information-requirements-relation-transfers-funds-and-certain-crypto-assets-transfers

there is a large and emerging regulatory framework for crypto-assets, significant aspects of the sector remain unregulated as outlined in vulnerability 6.

The global market capitalisation of crypto-assets represented an average of 1.2% of global GDP in 2023, while in 2024, this had nearly doubled to an average of 2.3%, and hit a record 3% in November 2024,[221] albeit some of this growth is attributed to price volatility.

Threats and Vulnerabilities

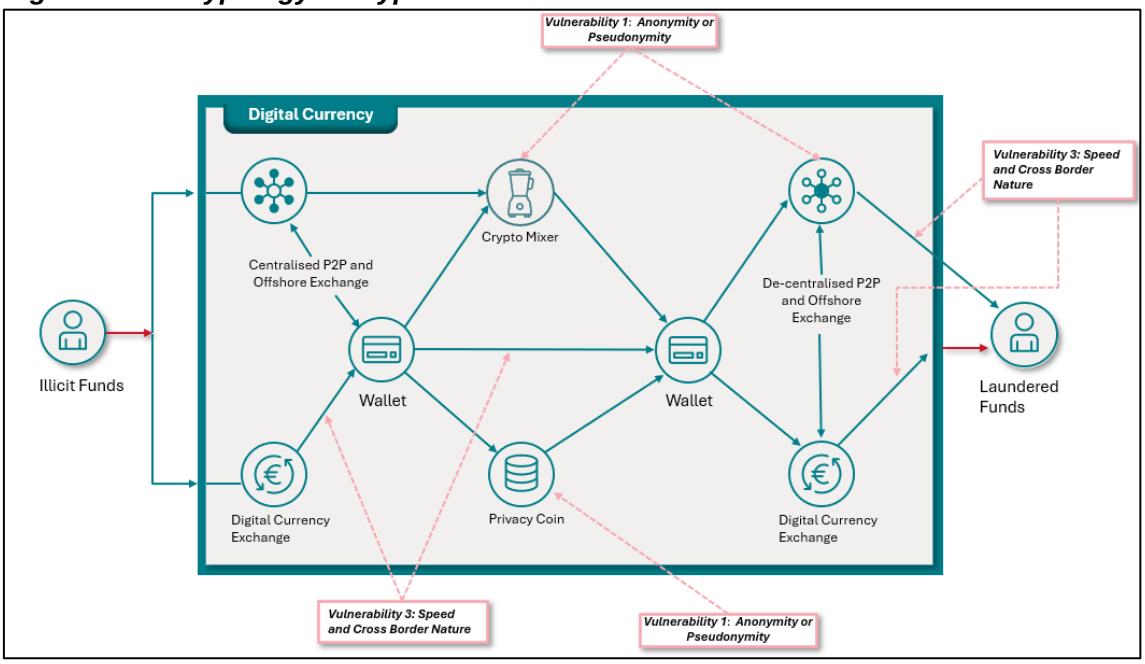
Threats

For more information, please refer to the crypto-assets section.

Vulnerabilities

This section outlines the primary vulnerabilities identified within the crypto-assets sector in Ireland. Understanding these vulnerabilities is crucial for developing effective risk mitigation strategies and ensuring the integrity of the crypto-asset ecosystem. The following ML typology involving the crypto-assets sector illustrates the vulnerabilities outlined below.

Figure 10: ML typology in crypto-assets



[221] Voronoi App / Cryptocurrency Market Cap Hits Record 3% of Global GDP in 2024 / Available from: https://www.voronoiapp.com/markets/-Cryptocurrency-Market-Cap-Hits-Record-30-of-Global-GDP-in-2024-3820

Vulnerability 1: Anonymity or Pseudonymity

In the crypto-assets sector, pseudonymity or anonymity is a feature that can present substantial risks related to ML/TF/PF.[222] The use of pseudonymous identities or anonymous wallets can conceal the true identities of the transaction parties, making it difficult for authorities to trace the movement of funds and detect illicit activities, and for counterparties in transactions to understand the risks of their transactional activity.

This vulnerability is heightened by the decentralised nature of many crypto-asset networks, which enable transactions to occur directly between users, bypassing traditional intermediaries like banks, brokerages, or exchanges. Added to this, CASP products and services are offered on a remote basis, which, combined with the higher-risk nature of the assets, can generate additional risk. While law enforcement and regulatory authorities can trace transactions on the blockchain, the level of traceability can vary significantly across products. For example, transactions on public blockchains, such as those involving non-fungible tokens or major cryptocurrencies, are often transparent and traceable using blockchain analytics tools. However, the absence of intermediaries often poses challenges for the identification and investigation of criminal transactions by law enforcement. Additionally, the rise of PETs such as mixing and tumbling services and privacy coins further complicates this process, as they are intentionally designed to obscure transactional data, presenting substantially higher risk. Such practices complicate CDD efforts, particularly in relation to source of funds verification and transaction monitoring, as assets may have been anonymised before entering the regulated environment.

Pre-MiCAR, the Central Bank imposed specific registration conditions on Irish-regulated VASPs, aiming to mitigate the risk of the use or facilitation of privacy coins or similar technologies designed to obscure the origin, flow, or destination of crypto-assets. However, transactions could have been subject to PETs before they transacted with a Central Bank registered VASP. Under MiCAR, trading platforms for crypto-assets are required to prevent the admission to trading of crypto-assets that have an inbuilt anonymisation function unless the holders of those crypto-assets and their transaction history can be identified by the CASP operating the platform.

[222] Financial Action Task Force / Updated Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers / 2021/ Available from: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.inline.pdf / p.18

Vulnerability 2: Inconsistent International Regulations

While MiCAR provides a collective European response, the global AML/CFT landscape for CASPs remains highly fragmented, with significant disparities in regulatory maturity, enforcement capacity, and legal frameworks across jurisdictions. This inconsistency undermines the effectiveness of international standards such as the FATF Travel Rule, which requires CASPs to collect and share originator and beneficiary information for crypto-asset transfers. As noted by FATF, nearly one-third of jurisdictions (32 out of 117) have not implemented the Travel Rule. Even among those that have, enforcement and supervision remain limited.[223]

Irish-regulated CASPs – which are required to apply the Travel Rule – may engage in cross-border transactions with counterparties in countries where Travel Rule implementation is weak or absent. This can directly affect the ability of Irish-regulated CASPs to meet their own regulatory obligations, particularly for use cases such as wallet-to-wallet transfers with a CASP in a country that has not fully implemented the Travel Rule, and where they are unable to obtain or verify required originator and beneficiary information. These gaps create compliance challenges—specifically, the inability to obtain originator and beneficiary data in a timely or verifiable manner, thereby undermining compliance, particularly in high-risk or high-value transactions. This exposes Irish-regulated CASPs to increased risk when transacting with offshore or unregistered CASPs. In addition, non-EU VASPs (and other operators in the sector who would be subject to ML/TF regulation in Ireland and the EU) can operate with limited oversight in some jurisdictions, making it easier for illicit actors to exploit these gaps.

Four years after FATF extended its global AML/CFT standards on crypto-assets and VASPs, global implementation of these standards was found to be inadequate, with three-quarters of jurisdictions Partially Compliant or Non-Compliant.[224] This global inconsistency enables VASPs licensed in lightly regulated or unregulated jurisdictions to offer services directly or indirectly in Ireland without falling under the supervision of the Central Bank. Such regulatory gaps are exploited by criminal actors, who seek out weaker regimes to facilitate illicit financial flows, increasing the risk of ML, TF, and PF exposure within the Irish financial system. However, there has been a growing trend toward a more rigorous supervisory approach in several jurisdictions around the world. For example, authorities in multiple countries have taken action against VASPs for ML and sanctions related breaches, and in the US there have

[223] FATF / Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers / Available from: https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2025-Targeted-Upate-VA-VASPs.pdf.coredownload.pdf / p.32
[224] Ibid. / p.32

been criminal charges brought against both firms and individuals involved in these breaches.[225]

As noted above, MiCAR has created a unified regulatory framework for crypto-assets across the EU (including AML/CFT obligations)[226] and reduces the inconsistencies and gaps that have existed between member states. This harmonisation will – for example – ensure that CASPs and issuers of ARTs and EMTs operate under the same set of regulations, and enhance the ability of firms operating in the EU to implement a consistent AML/CFT framework. Additionally, MiCAR's direct applicability across all EU countries minimises fragmentation, fostering a more cohesive and stable regulatory environment.

Vulnerability 3: Speed and Cross-Border Transaction Risk

The ability to quickly move large sums of crypto-assets across borders, as well as the near-instant and irreversible nature of these transactions, poses risks in terms of the immediacy of illicit transactions being completed before they can be detected by authorities. This variability makes it difficult for CASPs and regulators to implement effective transaction monitoring systems capable of identifying potentially illicit activities in real-time. This is especially relevant for Irish-regulated CASPs in cross-border transaction scenarios where regulatory standards and expectations may differ. However, instant payments have been the norm within SEPA since October 2025. Therefore, the speed advantage of crypto-asset settlement is more pronounced for transactions outside Europe.

There are characteristics of blockchain technology, such as its decentralised nature, cryptographic hashing, consensus mechanisms and transaction immutability, that facilitate effective transaction monitoring of crypto-asset transfers. The transparent, immutable, and timestamped nature of blockchain records enables detailed audit trails and forensic tracing of transactions, even across complex chains of activity. Advanced blockchain analytics tools have the potential to de-anonymise transactional flows, detect unusual patterns, and link wallet addresses to real-world actors over time. These capabilities – where deployed effectively and tailored to the risk profile of the firm – enhance the effectiveness of AML/CFT monitoring by allowing CASPs and regulators to detect suspicious behaviours that may be hidden in traditional finance. In particular, blockchain analytics can support early detection of typologies such as layering, cross-chain movement, or interaction with sanctioned

[225] US Department of Justice / Binance and CEO Plead Guilty Federal Charges / Available from: https://www.justice.gov/archives/opa/pr/binance-and-ceo-plead-guilty-federal-charges-4b-resolution#:~:text=As%20part%20of%20the%20plea,total%20financial%20penalty%20of%20%244%2C316%2C126%2C163
[226] European Council / Council of the European Union / Press Release / Digital Finance: Council Adopts New Rules on Markets in Crypto-Assets (MiCA) / Available from: https://www.consilium.europa.eu/en/press/press-releases/2023/05/16/digital-finance-council-adopts-new-rules-on-markets-in-crypto-assets-mica/

addresses, if paired with robust off-chain data sources and regulatory collaboration. However, while blockchain provides visibility into the flow of transactions, linking wallet addresses to specific beneficiaries remains a challenge, and in some forms of crypto-asset products and transactions the beneficial owners may be unknown. This is why regulated entry and exit points (e.g., banks and EMIs) remain crucial for the tracking and blocking of illicit funds.

Vulnerability 4: Complexity and Rapid Evolution of Products and Services

The crypto-assets sector's diverse range of products and services, along with the rapid development of new technologies, introduces various vulnerabilities. Tokens, stablecoins, mixers, tumblers, atomic swaps, layer-2 networks, and DeFi platforms each present unique risks. Technologies such as mixers and tumblers complicate fund tracing by consolidating multiple transactions, while atomic swaps facilitate cryptocurrency exchanges across different blockchains without a central exchange. As these technologies evolve, they increase the complexity of the crypto-asset ecosystem, necessitating that Irish-regulated CASPs regularly update their risk assessments and control frameworks. Many emerging products, particularly in DeFi and new token types, currently lack regulation, posing significant AML/CFT risks.

Additionally, certain crypto-asset services enable users to conduct complex financial transactions directly with one another, bypassing traditional intermediaries and regulatory oversight. While this decentralisation fosters innovation, it also presents challenges in tracking transactions, making it easier for criminals to exploit these systems for illicit activities.

Vulnerability 5: Resourcing, Outsourcing, and Intelligence Gaps

Due to the specialised knowledge required to work in the sector, it may be more difficult to employ skilled risk and compliance staff (including senior management) with the relevant experience in both the underlying technology and the AML/CFT expertise needed to effectively mitigate ML, TF, and PF risks.

Many CASPs in Ireland, particularly global firms using Ireland as their EU hub, rely on AML/CFT functions and resources in their wider group structure. If the frameworks implemented by these group entities are not tailored to the Irish legal, regulatory and risk context, it can lead to misaligned risk controls and reduced effectiveness of local AML/CFT frameworks. The Central Bank has seen evidence of gaps in the ML, TF, and PF control frameworks employed by VASPs which can in part be attributed to these factors, as well as sector-wide shortages of AML professionals with crypto-asset specific experience.

The limited exchange of information between CASPs and traditional financial institutions also presents challenges in identifying and addressing ML/TF/PF activities. Without effective frameworks for collaboration, this limits the sector's ability to detect suspicious patterns and mitigate risks. Additionally, the lack of structured intelligence-sharing mechanisms between CASPs and traditional banks limits coordinated detection of emerging threats and typologies.

Vulnerability 6: Unregulated Area of Crypto-assets

Unregulated areas within the crypto-assets sector, including in Ireland, may pose risks to the financial system. A major concern is DeFi, which allows individuals to conduct transactions directly without traditional intermediaries like banks, bypassing traditional identity verification through smart contracts on the blockchain.

Another unregulated activity is P2P transactions, where users exchange or trade crypto-assets directly, such as transferring assets between un-hosted wallets. While some platforms facilitating these transactions must comply with MiCAR, they can only trace transactions rather than intercept them, limiting their ability to prevent illicit activities. Initial Coin Offerings and Non-Fungible Tokens also operate in a largely unregulated environment. While DeFi and P2P platforms largely operate outside traditional regulatory frameworks,[227] international bodies like the FATF and the EU are exploring measures to incorporate these activities into AML/CFT regulations.

In contrast, stablecoins are subject to regulation under MiCAR, which imposes specific requirements on issuers and service providers, enhancing oversight and consumer protection.

Firms not authorised as CASPs in the EU can still provide crypto-asset services to Irish-based customers on a reverse solicitation basis (i.e. where the services are sought by the customer). These non-EU entities are not subject to the obligations imposed on MiCAR-authorised CASPs and are not subject to Central Bank supervision, posing risks as to the adequacy of their AML/CFT frameworks.

[227] Central Bank of Ireland / The evolving crypto landscape - towards the implementation of MiCA" - Remarks by Gerry Cross, Director of Financial Regulation, Policy & Risk / Available from: https://www.centralbank.ie/news/article/the-evolving-crypto-landscape-towards-the-implementation-of-mica-remarks-by-gerry-cross-30-may-2023

Case Study: Coinbase Settlement

In November 2025, the Central Bank of Ireland fined Coinbase Europe Limited (Coinbase Europe), a VASP, €21.46 million for breaching its AML/CFT obligations under the CJA 2010 with respect to transaction monitoring.

Coinbase Europe, which is part of the Coinbase Group, provides crypto-asset and wallet services to customers globally to facilitate their use of the Coinbase Group's trading platform to buy and sell crypto-assets. Under the CJA 2010, Coinbase Europe is required to monitor customer transactions on an ongoing basis and, where it suspects that a transaction is facilitating ML or TF, to file a Suspicious Transaction Report (STR) with the FIU and Revenue as soon as possible.

Between 23 April 2021 and 29 April 2022, Coinbase Europe's transaction monitoring system (TMS) did not operate properly, which resulted in it failing to properly monitor approximately 30 million transactions (the Non-Monitored Transactions) for certain high-risk scenarios that took place. The Non-Monitored Transactions amounted to approximately 31% of Coinbase Europe's total transactions over that period. Those transactions were valued at approximately €176 billion.

Coinbase Inc. (the parent company to whom transaction monitoring was outsourced) had to rescreen the Non-Monitored Transactions for the high-risk scenarios originally not captured by the TMS. This step was completed by August 2022, and 184,790 transactions were identified as requiring further review. Coinbase Inc. then had to investigate the alerts, ultimately resulting in Coinbase Europe submitting 2,708 STRs to the FIU and Revenue.

These STRs included transactions flagged by TMS as having reasonable grounds for suspecting ML, including for being potentially associated with the following: the darknet; controlled substances; illegal media services; malware; ransomware; scams; theft; child sexual abuse material; and OFAC tags. Coinbase Europe offboarded some of the related customers due to their engagement in suspicious transactions.

The last STR was filed on 28 January 2025, meaning the delay in reporting suspicious transactions stretched from several months to over three years from when the transaction occurred, undermining the efficacy of the STRs ultimately submitted.

The Central Bank also found that Coinbase Europe delayed in notifying it of the TMS failures between May and November 2023. This delay in notification was treated as an aggravating feature in the calculation of the monetary penalty, increasing it by 5%.

Consequence

Ireland's crypto-assets sector has grown, with increasing integration into both domestic and international financial systems. A material ML, TF or PF incident in this sector would have a broad impact on Ireland's financial system and its reputation in international financial markets. As such, the consequence has been rated as very significant.

EU Supranational Risk Assessment

The EU Supranational Risk Assessment assessed the crypto-assets sector in its most recent (2022) risk assessment as per the below:

TF Risk	ML Risk
Very Significant	Very Significant

The risk factors identified within this sectoral risk assessment are aligned with those set out in the EU Supranational Risk Assessment.

Horizon Scanning

As the CASP sector continues to evolve, several emerging trends and technologies present new opportunities as well as potential risks for ML, TF, and PF. These developments are reshaping the landscape for CASPs, regulators, and law enforcement.

Tokenisation of Real-World Assets

The tokenisation of traditional assets, such as real estate, commodities, and bonds, is increasingly gaining traction within the crypto-assets sector. Tokenisation allows the digital representation of real-world assets on blockchain networks, which can enhance liquidity, improve market access, and reduce transaction costs. However, this innovation also brings new risks related to the valuation, ownership, and transfer of tokenised assets, especially regarding their potential misuse for ML, TF or PF. The ability to fractionalise high-value assets may increase the ease of conducting illicit transactions, thereby raising concerns about transparency and compliance with existing AML/CFT obligations.

Cross-Chain Interoperability and Bridges

Cross-chain interoperability, which enables crypto-assets to move seamlessly between different blockchain networks, enhances operational efficiency within the sector. However, it also introduces new risks, as the ability to transfer assets across blockchains makes it harder

to trace the movement of funds, especially on DeFi and P2P platforms. Cross-chain bridges facilitate the transfer of assets from one blockchain to another, which can further obscure the origin and destination of funds.

Synthetic Identities and Artificial Intelligence-Generated ID Documents

The use of synthetic identities, created by combining real and fake data, is an emerging threat that undermines onboarding and customer verification controls. AI-generated identity documents are being used to bypass traditional KYC processes, which could potentially facilitate the creation of fraudulent accounts.

Payment Institutions and E-Money Institutions

Executive Summary

	2019 Risk Ratings	2026 Risk Ratings
E-Money Institutions		
ML	Not Assessed	Very Significant
TF	Not Assessed	Significant
PF	Not Assessed	Low
Money Remittance Firms		
ML	High	Very Significant
TF	High	Very Significant
PF	Not Assessed	Low
Payment Institutions (PIs) (other than Money Remittance Firms)		
ML	Medium-Low	Moderate
TF	Medium-Low	Moderate
PF	Not Assessed	Low

Key Insights

The PI and EMI sector in Ireland continues to grow, with increases both in the number and variety of firms entering the sector, as well as in the population's adoption and use of PI and EMI products and services.

The risk that PIs and EMIs facilitate ML and TF varies by sub-sector (see 'Scale and Structure' section for an explanation of these sub-sectors). However, it is generally higher in EMIs and Money Remittance firms. PF is rated as low for the sector, primarily due to the typically low value of individual transactions facilitated in the sector, and the lack of direct exposure to countries of proliferation concern.

The key vulnerabilities in the sector are:

- **Speed and cross-border nature of transactions:** The rapid transfer of funds enabled by PIs and EMIs can allow criminals to quickly move funds both across accounts as well as internationally, and can increase the inherent risks of illicit financial flows.

- **Widespread Adoption and Use of PI and EMI products:** PI and EMI services are increasingly widely adopted by and used in Ireland and offer a gateway to the financial system.

- **CDD thresholds and exclusions:** The ability to use some PI and EMI products without full due diligence requirements, such as identification and verification, increases the vulnerability in the sector.

- **Use of cash:** Despite the overall decline in the use of cash in Ireland, cash-based ML is a key risk for Money Remittance firms which accept cash as payment for remittance services, and some EMIs.

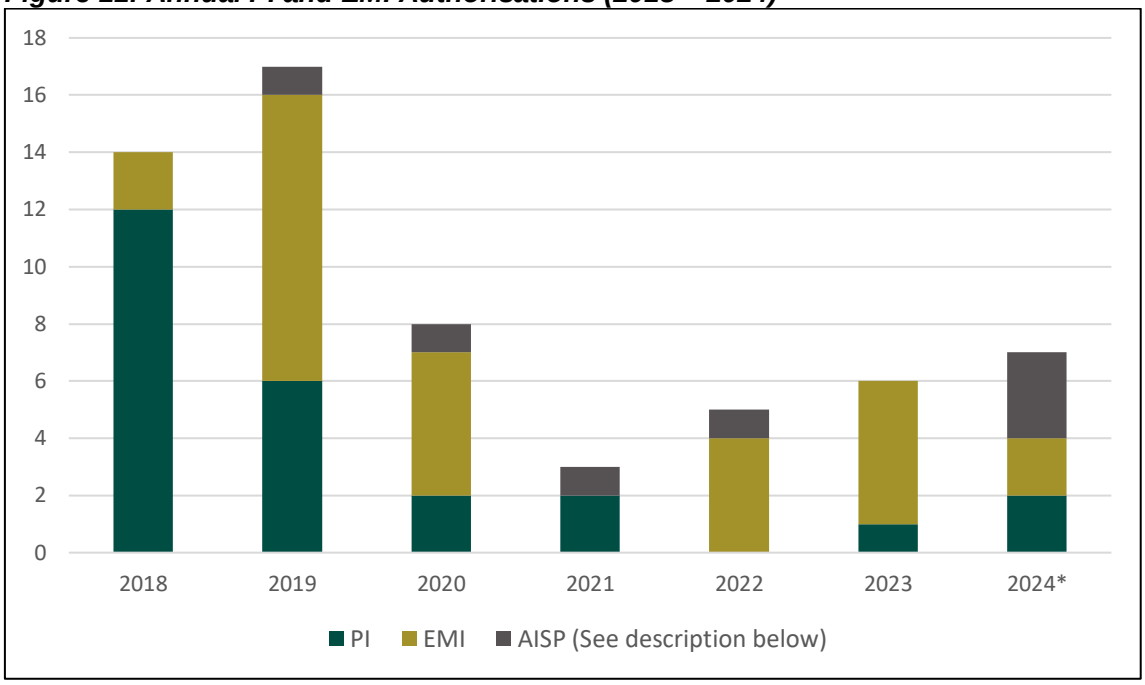
- **Use of agents and distributors:** Some Money Remittance and EMI firms use networks of agents and distributors to deliver their products and services and may rely on these parties to conduct AML and CFT controls (e.g. collection of CDD). Where oversight of these third parties is inadequate, this can lead to gaps in the controls executed on behalf of the PI and EMI firms, and further elevate the products and services exposure to misuse by criminals.

Scale and Structure of the PI and EMI Sector in Ireland

Ireland has a diverse ecosystem of PIs which are authorised under the Payment Services Directive 2 ("PSD2") to provide various payment services, as listed in Annex I of the Directive. As of December 2025, there are 23 authorised PIs. Out of these PIs, eight hold a licence that includes Money Remittance services. There are 28 authorised EMIs[228] in Ireland, of which five hold a licence that includes Money Remittance services. In addition, PIs and EMIs authorised in other EU jurisdictions can offer services to Irish residents under passporting rules. The majority of recent applications come from large groups aiming to establish Irish subsidiaries, with many seeking to use the subsidiary to 'passport out' services to other EEA countries. As shown in Figure 11, there was a significant increase in authorisation applications post-Brexit, with 18 new PI and 12 EMI authorisations during 2018 and 2019.[229]

[228] Central Bank of Ireland data
[229] Central Bank / Brexit Task Force Report January 2020 / Available from: https://www.centralbank.ie/docs/default-source/publications/brexit-working-group-reports/brexit-task-force-report-january-2020.pdf?sfvrsn=6b48871d_4

Figure 11: Annual PI and EMI Authorisations (2018 – 2024)[230]



*This illustration contains only the new authorisations, not the total number of authorised firms in the sector

There has also been increased adoption of digital and mobile payments in Ireland. As noted in the 2022 ECB report on stakeholder perspectives for a digital euro,[231] Ireland is a 'technologically mature' market, and mobile payments and other new and innovative payment methods are more widely used in such markets, particularly among younger users. The value of payments processed through the sector continued to grow in 2024, reaching €613 billion, an increase of 17% compared to 2023.[232] In addition to the ML, TF, and PF risks that the sector is exposed to (as outlined in this chapter), the PI and EMI sector also has a significant exposure to being used to facilitate fraud, including through the fraudulent issuance of payment orders, chargeback fraud, and manipulation of payer. The sector comprises three main sub-sectors, as described below.

[230] Central Bank of Ireland data
[231] European Central Bank / Study on New Digital Payment Methods / Available from: https://www.ecb.europa.eu/euro/digital_euro/timeline/profuse/shared/pdf//ecb.dedocs220330_report.en.pdf / p.8
[232] Central Bank of Ireland / Regulatory and Supervisory Outlook Report 2025 / Available from: https://www.centralbank.ie/docs/default-source/publications/regulatory-and-supervisory-outlook-reports/regulatory-supervisory-outlook-report-2025.pdf?sfvrsn=e185651a_5 / p.69

Payment Institutions: Money Remittance

Money Remittance firms are authorised under PSD2 to provide services as defined in Article 4(22).[233] Firms in this sector are diverse and range from individual businesses to complex firms with expansive networks of branches and agents. 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. These firms transmit funds on behalf of a payer to a payee, without creating a payment account for either party with the sole purpose of transferring funds. These firms can facilitate the transfer of funds, both domestically and internationally, on behalf of both individuals and businesses, using multiple currencies. Services are typically delivered through digital platforms, mobile applications or agent networks. A quarter of these firms' operations and customer bases are exclusively within Ireland, ≈37% limited to the EEA, and ≈38% have operations and customer bases outside of the EEA.[234] While Money Remittance services have traditionally been associated with unbanked populations, customers are increasingly using these services alongside their Retail Banking services.

Payment Institutions: Other than Money Remitters

Firms authorised under PSD2 to provide payment services as listed in Annex I, excluding money remittance. These include, but are not limited to, services involving the operation of a payment account, execution of credit transfers and direct debits, issuing or acquiring of payment instruments and services offered by Payment Initiation Service Provider and Account Information Service Providers. While currency exchange services were listed in the previous NRA, they are now considered ancillary to broader payment services rather than standalone services.[235] Similarly, debt management services were referenced in the last NRA but are not considered payment services under the regulations.[236] Of the firms in this sector, 10% have fully domestic operations and customer bases, 60% of firms have operations and customer bases fully within the EEA, and 30% have operations and customer bases outside of the EEA.[237]

[233] Directive (EU) 2015/2366, Article 4(22) - Money Remittance
[234] Central Bank of Ireland data
[235] Central Bank of Ireland/ Money Transmission Businesses / Available from: https://www.centralbank.ie/regulation/industry-market-sectors/money-transmission-businesses
[236] Central Bank of Ireland / Debt Management Firms / Available from: https://www.centralbank.ie/regulation/industry-market-sectors/debt-management-firms
[237] Central Bank of Ireland data

E-Money Institutions

EMIs are authorised to issue electronic money, as defined in Directive 2009/110/EC ("EMD2") Article 2(2).[238] These firms issue electronically stored monetary value upon receipt of funds, which represents a claim on the issuer and is accepted by persons other than the issuer. This product can, like PI products under the PSD2, facilitate payment transactions including through prepaid cards, digital wallets or similar instruments.

The development and provision of e-money can involve Issuers, Agents and Distributors.

- **E-Money Issuer:** An undertaking that has been authorised to issue e-money in accordance with the E-Money Directive.

- **Agent:** Provides payment services as well as distributing and/or redeeming e-money; e-money agents are not permitted to issue e-money.

- **Distributor:** Can distribute and/or redeem e-money but cannot provide payment services. Distributors may be unregulated and might include retail businesses (e.g. pre-paid cards sold in retail outlets).

Across the sector, 68% of firms have operations and customer bases limited to the EEA, while the remaining 32% have operations and customer bases outside of the EEA.[239]

Threats and Vulnerabilities

Threats

The ML, TF, and PF threats to which Ireland is exposed are assessed above. The PI and EMI sector faces significant threats from OCGs, fraudsters, and terrorist networks seeking to exploit the sector's digital and cross-border payment infrastructure. These actors use PI and EMI services to facilitate the rapid movement and layering of illicit funds, capitalising on the speed and high volume of transactions to evade detection by authorities. Fraud schemes targeting both consumer and business customers, including identity theft and account takeovers, are also increasingly prevalent. Informal money remittance services, such as hawala and similar networks, are also extensively used by OCGs to move funds, bypassing regulated channels.

[238] Directive (EU) 2009/110, Article 2(2)
[239] Central Bank of Ireland data

A total of 25,166 (3,703 STRs[240] and 21,463 STReu[241]) STRs were submitted by firms in this sector in 2024. Of those which have been fully analysed, ≈23% were disseminated; ≈4% to law enforcement within Ireland and ≈19% to other FIUs. In 99% of the 25,166 STRs submitted, ML was cited as an indicator.

Vulnerabilities

In assessing the vulnerabilities of the PI and EMI sector in Ireland to ML, TF, and PF threats, this risk assessment has considered EBA[242] and FATF[243] guidance and the results of the EU Supranational Risk Assessment. The scale, structure and nature of the payments sector in Ireland has also been assessed, including the extent to which the payments sector has implemented proportionate controls to mitigate the identified threats.

Vulnerability 1: Speed and Cross-Border Nature of Transactions

The rapid transfer of funds enabled by PIs and EMIs can allow criminals to quickly move funds both across accounts as well as internationally, and can increase the inherent risk of illicit financial flows.

The speed and cross-border nature of transactions within the sector can complicate the detection, reporting and investigation by law enforcement of suspicious activity. This can be further exacerbated where transactions involve jurisdictions which have lower regulatory standards, or jurisdictions with limited frameworks for sharing information internationally (for instance through MLA channels).

The EBA report on ML and TF risks[244] identified geographical risk as a significant concern within the Money Remitters sub-sector. This risk is particularly heightened where transactions are being processed to high-risk third countries. Although Irish PIs and EMIs do have a substantial international exposure, operations and customers are largely in EEA countries. Only one PI/EMI firm had a high-risk third country in its top 5 countries for

[240] Designation is selected by the entity at registration.
[241] STReu is a specific report, usually submitted by entities located in Ireland and passporting their services to other EU countries, where there is no nexus to Ireland. All 21,463 of these reports have been processed and disseminated to the relevant EU FIU.
[242]European Banking Authority / Final Report on Guidelines on Revised Money Laundering /Terrorist Financing Risk Factors / Available from: https://eba.europa.eu/sites/default/files/document_library/Publications/Guidelines/2021/963637/Final%20Report%20on%20Guidelines%20on%20revised%20ML%20TF%20Risk%20Factors.pdf
[243] Financial Action Task Force / FATF Recommendations 2012 / Available from: https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf
[244]European Banking Authority / Report on Money Laundering /Terrorist Financing Risks Associated with Payment Institutions / 2023 / Available from: https://www.eba.europa.eu/sites/default/files/document_library/Publications/Reports/2023/1056453/Report%20on%20ML%20TF%20risks%20associated%20with%20payment%20institutions.pdf

operations and customer base, and there is no known direct exposure to countries of concern from a PF perspective.[245] This combination of factors means that, in the Irish context, the inherent exposure for cross-border transactions is reduced due to the limited direct exposure to high-risk third countries.

These risks can be mitigated through the implementation of effective controls by firms in the sector. However, the Central Bank has noted that controls in PI and EMI firms are not as robust as they should be and are not commensurate with the risk exposure in the sector.[246] The Central Bank has identified weaknesses[247] in transaction monitoring control, which is a key control in mitigating the risks associated with cross-border transactional activity.

Vulnerability 2: Widespread Adoption and Use of PI and EMI products

Access to PI and EMI products and services can be obtained with relative ease and are increasingly widely adopted in Ireland – for instance through a 'brick-and-mortar' retail location, or through digital platforms. PI and EMI firms are increasingly offering products and services which are similar in nature to those offered by Retail Banks; there are therefore similar vulnerabilities, as some of these products and services provide a gateway into the financial system, with products that are both essential for legitimate activity and susceptible to criminal misuse. However, certain EMI products – such as non-reloadable gift cards – present a lower level of risk, due to the limits on the value of transactional activity which they permit.

P2P transactions and Money Remittance services are widely adopted, and particularly susceptible to misuse, including as these products can move funds quickly, often internationally, and can in some cases accept cash. Prepaid cards and e-wallets also pose risks due to their potential for anonymity, acceptance of cash, reloadability, and cross-jurisdictional use. Where these products and services are funded by bank transfer, this may lower the inherent risk given that the funds are being sent from other regulated firms; whereas cash payments accepted by Agents of Money Remittance firms are likely to pose heightened risks. For the PI – Others sub-sector, widespread use is less likely to be a vulnerability; for

[245] Central Bank of Ireland data
[246] Central Bank / Regulatory and Supervisory Outlook Report 2025 / Available from: https://www.centralbank.ie/docs/default-source/publications/regulatory-and-supervisory-outlook-reports/regulatory-supervisory-outlook-report-2025.pdf?sfvrsn=e185651a_9 / p.66
[247] Central Bank / Dear CEO Letter: Supervisory Findings and Expectations for Payment and Electronic Money Firms / Available from: https://www.centralbank.ie/docs/default-source/regulation/industry-market-sectors/payment-institutions/dear-ceo-letter-supervisory-findings-and-expectations-for-payment-and-electronic-money-firms.pdf?sfvrsn=408d981d_3

instance, the widespread use of Account Information Service Providers would not necessarily result in heightened risk, given their limited risk profile.

Vulnerability 3: CDD Thresholds and Exclusions

Some PI and EMI products can present heightened vulnerability, including where they fall below thresholds or are subject to a lower level of CDD. These services can be provided on a one-off or occasional basis, where the standard due diligence requirements are not applied; this has been identified as a key risk factor by AML/CFT supervisors across EU member states.[248] The risk is especially pronounced in the remittance sub-sector, where average transaction values tend to be small, meaning that identification and verification requirements may not always be required, potentially creating opportunities that criminals can exploit for ML, TF, and PF activities.

This vulnerability is heightened for EMIs where cards, wallets or accounts are reloadable, where they can be funded by third parties, and for PI Money Remitters where there can be challenges in being able to 'link' occasional transactions or activity by the same underlying customer. There are also heightened risks where the product or service can be funded by cash, as this can inhibit the ability of the PI/EMI to understand source of funds, compared to where the product is purchased by (for example) bank transfer. Please refer to the ML typology section for more context on cash-based ML typologies.

Law enforcement has noted a growing trend of prepaid cards being used by criminal organisations, including as a means of payment for low-value amounts to criminal associates. This type of activity will likely be subject to both limited monitoring and little due diligence by the regulated firms.

Vulnerability 4: Use of Cash

Cash-based ML remains a vulnerability for PIs with Money Remittance services (particularly those which use 'brick and mortar' agent locations and retail outlets to facilitate transactional activity), with this sector being noted as the most efficient mechanism for sending cash internationally.[249] These firms are therefore exposed to common cash-based ML and TF

[248] European Banking Authority / Report on Money Laundering/Terrorist Financing Risks Associated with Payment Institutions / 2023 / Available from: https://www.eba.europa.eu/sites/default/files/document_library/Publications/Reports/2023/1056453/Report%20on%20ML%20TF%20risks%20associated%20with%20payment%20institutions.pdf / p.9
[249] Ibid. / p.10

typologies, including structuring transactions to avoid reporting thresholds, use of cash as a source of funds for transfers to high-risk jurisdictions, and money muling.

EMIs offering reloadable prepaid cards and digital wallets can also act as cash entry points, particularly through the purchase of vouchers or retail top-ups. These products have been used by criminal groups, as outlined in ML and TF threat assessments.

In contrast to this, PIs that do not provide Money Remittance services, such as those only offering payment initiation or account information services, have very limited exposure to cash as a vulnerability, as they operate in digital environments, often have no physical presence or agent networks and do not handle customer funds directly. Any residual exposure to cash stems indirectly from the underlying payment accounts accessed via their platforms, which may have been funded by cash deposits.

Vulnerability 5: Use of Agents and Distributors

Some PI – Money Remittance firms rely on agents to carry out transactions on behalf of customers, and EMIs may engage agents and distributors; these services are often offered as an ancillary activity to the main business of the agent or distributor. In both cases, these third parties can play a key role in implementing elements of the firm's control framework, including the collection of KYC documentation, and assisting with transaction monitoring. This can result in vulnerability, in instances in which there are gaps in oversight by the regulated firm of their agent / distributor network, or where an agent or distributor is knowingly facilitating ML or TF activities. This vulnerability has been noted by the Central Bank in its supervisory activities, and a January 2023 Central Bank issued 'Dear CEO letter'[250] raised concerns about weak oversight of agents and distributors, particularly when they perform AML/CFT tasks such as CDD.

Consequence

The Irish PI and EMI sector is a growing and increasingly important part of financial services in Ireland. PI and EMI products and services are widely adopted by individuals and businesses, are deeply integrated in the financial system in Ireland, and have a significant international focus. A substantial ML, TF or PF incident in this sector would impact users, the

[250] Central Bank / Supervisory Findings and Expectations for Payment and Electronic Money Firms / Available from: https://www.centralbank.ie/docs/default-source/regulation/industry-market-sectors/payment-institutions/dear-ceo-letter-supervisory-findings-and-expectations-for-payment-and-electronic-money-firms.pdf?sfvrsn=408d981d_3

wider public and undermine trust in the payments services industry and wider Irish economy, both domestically and internationally. As such, the consequence has been rated significant.

EU Supranational Risk Assessment

The EU Supranational Risk Assessment assessed the Payment and E-Money sector in its most recent (2022) risk assessment as per the below:

Sub-Sector	TF Risk	ML Risk
E-Money	Significant	Significant
Money Remittance	Very Significant	Significant
Payments	Significant	Significant

The risk factors identified within this sectoral risk assessment are aligned with those set out in the EU Supranational Risk Assessment.

Horizon Scanning

Instant Payments: The ongoing and staged implementation of Instant Payments requirements presents additional challenges in implementing ML, TF, and PF controls. Instant payments are now fully operational for both sending and receiving payments since October 2025. For firms in the regulated sector, this poses additional challenges to transaction monitoring and sanctions screening systems, including the ability to conduct 'real-time' monitoring arrangements and/or block illicit payments. From a law enforcement perspective, one of the primary challenges in combating illicit financial flows is the speed at which funds can now be transferred. Rapid transactions, especially those facilitated by digital platforms, can significantly hinder the ability to trace and ultimately seize illicit assets. Funds will be able to be moved even more swiftly between accounts and across jurisdictions, making tracing more difficult. Without timely intervention mechanisms, there is a substantial risk that illicit assets will be dissipated beyond reach.

Recent data from 18 National Crime Agencies across the EU shows that fraud rates for instant payments are, on average, ten times higher than those associated with conventional credit transfers. While these figures vary significantly by Member State, the EBA notes this as an early but important indicator of emerging risk. According to the EBA, one likely reason for the elevated fraud rates is that instant payments are processed within 10 seconds, making it difficult or impossible for payment service providers to recall funds once fraud is identified.

Additionally, technical limitations may restrict the effectiveness of transaction monitoring and intervention before the transaction is executed.[251]

Virtual IBANs: As outlined in the Retail Banking sectoral risk assessment, these instruments introduce specific ML/TF risks due to the potential anonymity of end users and associated challenges in CDD, transaction monitoring, and suspicious activity reporting. These considerations should be taken into account when assessing the Banking and PI/EMI SRAs.

Open banking: The types and volume of payment intermediaries[252] have increased due to the advent of open banking. The introduction of new payment intermediaries adds complexity in payment chains, and results in these intermediaries having to rely on ML, TF, and PF controls in other regulated institutions. In addition, as payment chains become more complex, this could inhibit the ability of regulated firms to understand end-to-end payment chains, thereby limiting the effectiveness of monitoring arrangements and controls to understand the purpose and nature of transactional activity.

Redefinition of E-Money: In January 2025, the European Commission clarified the meaning of e-money through the EBA's Q&A process (ID 2022-6336).[253] This ruling was influenced by the ECJ's ruling in case C-661/22,[254] which emphasised that e-money is a separate monetary asset, distinct from the funds received by the issuer. The European Commission clarified that for a product to qualify as e-money, it must be accepted by third parties as means of payment and not solely redeemed for funds with the issuer. This interpretation implies that acceptance requires a contractual agreement between the e-money issuer and the payee. Firms should reflect on the Q&A and consider any impact it may have on business models and consequently the ML/TF risk to which they are exposed.

[251] European Banking Authority / Opinion on New Types of Payment Fraud and Possible Mitigations / 2024 / Available from: https://www.eba.europa.eu/sites/default/files/2024-04/363649ff-27b4-4210-95a6-0a87c9e21272/Opinion%20on%20new%20types%20of%20payment%20fraud%20and%20possible%20mitigations.pdf / p.5
[252] Including Account Information Service Providers and Payment Initiation Service Provider
[253] European Banking Authority / Single Rule Book Q&A ID 20226336 / Available from: https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2022_6336
[254] Publications Office of the European Union / EUR-Lex - CELEX:62022CJ0661 / Available from: https://eur-lex.europa.eu/legal-content/EN/CASE/?uri=CELEX:62022CJ0661

Retail Credit Firms

Risk Rating

	2019 Risk Ratings	2026 Risk Ratings
ML	Not Assessed	Low
TF	Not Assessed	Low
PF	Not Assessed	Low

Profile of Sector

A Retail Credit Firm ("RCF") provides credit through products such as mortgages, personal loans, instalment plans, and credit cards. The retail credit sector in Ireland comprises 27 firms, serving approximately 295,000 customers as of December 2025. The sector's assets total just under €50 billion, with activities encompassing both secured and unsecured lending, collateralised by property and other assets. The top three firms account for over 60% of the customer base and 90% of total assets in the sector.

Threats

The primary ML threat in the retail credit sector stems from the early repayment of loans, which can sometimes be facilitated by third parties and used to obscure the source of the funds. Criminal actors may exploit this method to layer illicit funds, paying off loans prematurely in order to appear legitimate while avoiding scrutiny. Certain TF risks are also present in the sector, particularly in the form of small consumer loans being used to support low-cost or small-scale terrorist operations. While not a predominant typology, such risks are relevant in cases involving cross-border transactions or customers with links to conflict zones.

That said, the use of RCFs for ML or TF purposes is assessed to be limited according to available intelligence. The EBA has also noted in its AML/CFT Opinions that the retail credit sector typically does not feature high-risk products or services that attract criminal organisations on a large scale. However, evolving financial crime techniques could still exploit emerging weaknesses, particularly where repayment patterns or customer behaviour significantly deviate from institutional standards without adequate oversight.

Vulnerabilities

The retail credit sector's vulnerabilities lie in its relatively straightforward product offerings, which mean that laundering illicit funds requires little technical knowledge or sophistication.

These non-complex products, such as consumer loans and credit lines, can serve as a vehicle for ML when AML controls, including transaction monitoring systems, are not sufficiently robust. A further vulnerability arises from the practice of retail credit firms acquiring loan portfolios as assets from other lenders. In such cases, RCFs may not always have a complete understanding of the customer base associated with these assets, leaving gaps in CDD measures and potentially allowing suspicious clients or patterns of behaviour to go unnoticed.

Geographically, the retail credit sector is generally low-risk, as most firms primarily operate within Ireland, limiting exposure to higher-risk jurisdictions. However, vulnerabilities could escalate where loans are issued to borrowers with cross-border ties or where third-party intermediaries facilitate repayment. The EBA also highlights geographic risk as a consideration even within domestic contexts, particularly if supervised firms lack mechanisms to identify higher-risk borrowers tied to specific regions of concern.

Control Weaknesses

The quality of controls in this sector is inconsistent across firms. Despite the presence of AML/CFT frameworks, varying levels of weakness in a number of control areas have been identified, particularly in respect of AML/CFT governance, ML/TF risk assessment, monitoring and CDD. Notwithstanding the presence of documented policies and procedures, significant enhancements are required to demonstrate compliance. Engagements have identified a lack of alignment between documented ML/TF risk assessments and operational practices, insufficient qualitative and quantitative data in MLRO reports and inadequate evidence of Board engagement on AML/CFT matters. Usage of group documentation, not adequately tailored to meet firms' local legislative and regulatory obligations, has also been identified. Deficiencies identified also include a lack of adequate understanding by firms of the ML/TF risks faced, as many assessments are generic and not appropriately tailored to the firms' business models. Furthermore, inherent risks and associated controls have been poorly documented, with TF risks not adequately assessed in some cases. Monitoring deficiencies identified include a lack of alignment between risk assessments and monitoring conducted, which is often 'one-size-fits-all' and not appropriately tailored to the identified risks. A contributing factor in this regard can be a firm's inadequate knowledge of its customer base, due to a lack of comprehensive or appropriately updated CDD information and documentation.

Bureaux de Change

Risk Rating

	2019 Risk Ratings	2026 Risk Ratings
ML	High	Significant
TF	High	Moderate
PF	Not Assessed	Low

Profile of Sector

The bureau de change sector in Ireland consists of six authorised firms, serving approximately 700,000 customers in 2024. These firms primarily facilitate currency exchanges between euro and non-euro currencies, catering to a customer base that includes tourists, cross-border shoppers, workers, and traders. Over the past decade, the sector has contracted significantly, with both the number of firms and the volume of cash exchanged declining. This decline is driven by shifts in consumer preferences and a broader move away from cash in favour of card payments and digital transactions. Unlike banks, which offer currency exchange services to their own customers as part of a broader suite of financial offerings, bureaux de change operate as specialised providers focused solely on currency transactions. One large bureau de change firm operates mainly through the Credit Union network.

Threats

The primary threats to the bureau de change sector arise from its misuse by criminal actors during the layering stage of the ML process. This stage involves distancing illicit funds from their origin. The ease and anonymity these firms can provide, particularly in high-cash environments, make them vulnerable to exploitation by OCGs, potentially in border areas where smuggling activity is prolific. These groups often rely on the flexibility of currency exchange to move illicit proceeds across jurisdictions. In addition to ML risks, bureaux de change are also exposed to TF risk. The use of foreign currencies, such as US dollars, to fund terrorism in conflict zones is a recognised typology flagged by the EU Supranational Risk Assessment, which identifies the sector as high-risk for TF. Cash-based transactions facilitated by these firms can be exploited to finance terrorism, especially in contexts where cash portability is essential. However, while bureaux de change play a role in supporting cross-border financial transactions, they typically do not provide direct access to the formal financial system, which limits their involvement in some TF typologies.

Vulnerabilities

The bureau de change sector's vulnerabilities are due to the fact that it is a cash-intensive business model, whereby the majority of transactions are occasional with no established business relationships. The sector predominantly relies on face-to-face transactions, and the business model poses challenges for effective customer profiling, including identifying source of funds, understanding the purpose of the transaction, and identification of linked transactions. For currency exchange offered by Retail Banks and Credit Unions, this risk is mitigated by the fact that services are only offered to existing customers, where a business relationship has been established. Most bureau de change firms apply thresholds for transactions by value as a mitigant to ML/TF risk. In addition, the currency exchanged at a counter is not transferred anywhere and to integrate cash the customer will need another financial institution.

Control Weaknesses

Recent inspection activity has identified several control weaknesses in the AML/CFT frameworks of bureau de change firms, which remain particularly vulnerable due to their cash-intensive operations. Key issues include inadequate risk assessment frameworks, with many firms adopting generic approaches that do not effectively address the specific risks of their business models. Transaction monitoring processes are another area of concern, often relying excessively on manual intervention, which increases the risk of errors and reduces the effectiveness of identifying suspicious activity. Governance structures and AML/CFT training for employees are frequently found to be insufficient, limiting firms' ability to manage evolving financial crime risks effectively. Furthermore, widespread reliance on manual record-keeping adds operational vulnerabilities, particularly in high-volume environments, making compliance slow and less accurate. Addressing these issues requires investment in automated systems, stronger governance, and effective training to ensure these firms can meet regulatory expectations and mitigate inherent risks.

Life Insurance

Risk Rating

	2019 Risk Ratings	2026 Risk Ratings
ML	Medium-Low	Moderate
TF	Medium-Low	Low
PF	Not Assessed	Low

Profile of Sector

The life insurance sector in Ireland consists of 39 firms serving 20 million policies in force as of December 2024. It is divided between domestic providers focusing on products, such as protection, pensions and investments, and international insurers often offering higher-value, investment-linked products, aimed at cross-border clients. A significant number of firms operate outside Ireland, with many conducting business beyond the EEA, reflecting Ireland's role as a key hub for international insurance. This dual domestic and international focus highlights its diverse customer base and broad economic reach.

Threats

The primary ML threats to the life insurance sector stem from its potential misuse by organised crime, particularly through investment-linked products that feature significant surrender/partial surrender values. Such products allow for the rapid conversion of illicit funds into seemingly legitimate payouts, making them attractive for laundering purposes. The sector’s international scope further amplifies these risks, as it frequently deals with high-net-worth customers and cross-border activity, exposing firms to risks associated with PEPs and higher-risk clients. This is especially significant in non-EEA jurisdictions, with weaker AML/CFT frameworks, which may reduce the effectiveness of the controls in place to monitor or flag suspicious activity.

On the other hand, the sector faces limited exposure to TF threats due to the nature of life insurance products. Most policies are long-term with controlled payouts triggered by specific, verifiable events such as death or maturity, reducing their utility for TF schemes. Nevertheless, companies operating in this space should remain cautious, particularly when high-value products or international accounts are involved.

Vulnerabilities

The life insurance sector's vulnerabilities primarily arise from the characteristics of certain investment-linked products, particularly those which offer flexibility (e.g. partial surrenders without financial penalties) or which have significant cash surrender values, which can be exploited for ML. Such products allow criminals to integrate illicit funds into the financial system by investing in policies and quickly liquidating them for perceived legitimate payouts. The sector's international reach further magnifies its exposure to vulnerabilities.

As highlighted in the EU Supranational Risk Assessment ("SNRA"), the cross-border nature of the sector enables organised criminals to exploit regulatory gaps between jurisdictions, particularly where enforcement is less robust. The involvement of intermediaries in the distribution of high-value products also increases the likelihood of weakened controls, particularly when AML/CFT oversight is inadequate.

Control Weaknesses

Despite a generally good understanding of ML/TF risks and AML/CFT obligations, the life insurance sector faces notable areas for improvement in its control frameworks. Key weaknesses are evident in risk assessment processes and governance, particularly among firms with an international focus offering insurance products with investment features, which inherently carry higher ML/TF risks. These firms often fail to implement controls robust enough to reflect their elevated risk exposure.

Additionally, CDD processes represent another area requiring enhancement, especially in the identification and verification of beneficial owners and transaction patterns involving high-risk customers. However, firms have demonstrated a proactive attitude in addressing these deficiencies, engaging with supervisory feedback and showing a commitment to remediation. Improvements in governance, tailored risk assessments, and more effective CDD measures remain essential to align the sector's control frameworks with its identified risk exposure.

MiFID Investment Firms

Risk Rating

	2019 Risk Ratings	2026 Risk Ratings
ML	Not Assessed	Moderate
TF	Not Assessed	Low
PF	Not Assessed	Low

Profile of Sector

The MiFID investment firms[255] sector in Ireland comprises 91 firms as of December 2025, reflecting a highly diverse industry segmented into sub-sectors such as broker-dealers, asset management firms, and stockbrokers. These firms range from small, niche operators offering specialised services to large, globally connected institutions providing a wide array of investment products and solutions. This diversity allows the sector to cater to varying customer needs and demands across both domestic and international markets. Importantly, the diversity within the sector results in variation in both the risk levels and typologies to which individual firms are exposed.

The customer base served by these firms is equally varied, encompassing HNWIs seeking tailored wealth management strategies, retail customers accessing brokerage or advisory services, and institutional customers such as pension funds or corporates requiring investment management solutions. The range of products and services offered is broad, including stockbroking, asset management, wealth management, and investment advisory services, alongside more complex offerings such as structured financial instruments and trading platforms.

Threats

MiFID investment firms can be exposed to ML and TF threats due to the inherent complexity and the diverse range of financial instruments they handle. Financial products such as derivatives and structured instruments can provide opportunities to obscure the movement of illicit funds, enabling criminals and terrorist actors to exploit trading mechanisms. These

[255] The MiFID sector refers to firms authorised under the Markets in Financial Instruments Directive (MiFID II), which governs the provision of investment services in financial instruments such as shares, bonds, derivatives, and structured products. These firms include brokers, wealth managers, and investment firms that offer services like portfolio management, investment advice, and trading 1. MiFID firms are subject to detailed conduct, governance, and prudential requirements, with a focus on investor protection, transparency, and market integrity

threats may be exacerbated by geographic factors, with some firms exposed to cross-border transactions and international customers.

A further threat factor is the exposure of MiFID investment firms to customers using complex legal structures, such as trusts, multi-layered corporate entities, and SPVs, which can obscure ultimate beneficial ownership and hinder transparency.

The EU Supranational Risk Assessment classifies the investment firm sector as high-risk for ML due to its exposure to cross-border activity, offshore customers, and international financial flows, which can all be leveraged to facilitate ML and the placement or layering of funds. TF risks, while generally lower, arise from the nature of certain financial instruments that can be repurposed to transfer funds internationally, circumventing detection mechanisms. Exposure to PEPs and non-EEA customers may further amplify these threats, as highlighted in the EBA Opinion on ML/TF risks. As detailed above, in consideration of the sectoral diversity, some MiFID investment firms operating in Ireland will be more exposed to these risk factors than others.

Vulnerabilities

The vulnerabilities of the MiFID investment firms sector primarily stem from the complexity and scale of its operations, as well as the diversity of financial instruments offered. Some firms are exposed to fast-paced, high-volume transactions across multiple jurisdictions, requiring robust monitoring controls. These vulnerabilities are heightened where firms engage in higher-risk activities or maintain relationships with customers from jurisdictions with weaker AML/CFT frameworks. Firms should be cognisant of the EBA Opinion on ML/TF risks which states that key risk factors include the operational focus of firms outside the EEA and/or exposure to funds originating from offshore markets.

Another significant vulnerability arises from the use of intricate customer structures such as trusts, SPVs, and multi-layered corporates. These entities can obscure the ownership chain or the true purpose of transactions, requiring robust due diligence. The SNRA notes that the detection and mitigation of risks associated with beneficial ownership transparency remain key challenges for the investment sector. Similarly, exposure to PEPs and HNWIs, who may engage in wealth management services, necessitates enhanced controls due to the elevated risk of misuse.

Control Weaknesses

The MiFID investment firms sector demonstrates variable effectiveness in its AML/CFT systems and controls, with several areas requiring enhancement. A key area for focus includes transaction monitoring, specifically making sure processes keep pace with the risks which accompany high-speed trading and complex financial products to support the effective and timely detection of potentially suspicious activity.

A further area of focus is CDD processes, particularly when dealing with customers operating through complex ownership structures or cross-border arrangements. Governance frameworks equally require improvement, with a need for stronger oversight mechanisms and more comprehensive risk assessments to address the complexities inherent in this sector. Addressing these gaps through improved technological tools, tailored CDD measures, and enhanced governance structures will be critical to ensuring these firms can effectively manage ML/TF risk in their fast-evolving operational landscape.

MiFID Markets Firms

Risk Rating

	2019 Risk Ratings	2026 Risk Ratings
ML	Not Assessed	Moderate
TF	Not Assessed	Low
PF	Not Assessed	Low

Profile of Sector

The MiFID markets sector in Ireland comprises approximately 13 firms as of December 2025. Firms in this sector operate diverse business models including Ireland's sole market operator, which facilitates trading and settlement of financial instruments. The sector also includes firms operating trading venues across multiple asset classes and firms which are significant liquidity providers and/or market makers to securities markets and algorithmic and high-frequency trading firms. Lastly, the sector also includes proprietary trading firms trading stocks, bonds, currencies, commodities, their derivatives or other financial instruments with the firm's own money, or in line with the MiFID authorisation of 'Dealing on Own Account'.

Most firms in this sector share several attributes and characteristics, specifically: high volume and value transactions processed from predominantly regulated, institutional customers operating across a broad range of jurisdictions. Importantly, this sectoral diversity results in variation in both the risk levels and typologies to which individual firms are exposed.

Threats

MiFID markets firms face ML/TF threats, largely driven by the speed, complexity, and opacity of financial instruments and trading activities. These firms operate in trading environments that enable rapid and often high-value transactions, creating opportunities for criminals to layer their activities within the sheer volume and velocity of transactions. The complexity of certain financial instruments including derivatives, options, and other structured financial instruments can further mask illicit transactions, providing a mechanism for layering and obfuscating the movement of illicit funds. Criminal actors may exploit these mechanisms to layer funds across the financial system or transfer them across jurisdictions with limited traceability.

The globalised nature of MiFID markets firms may compound these risks, as they often facilitate cross-border transactions and cater to a geographically diverse customer base. However, it is important to note the customer base predominantly comprises regulated institutional customers. According to the SNRA, markets firms, particularly those engaging in cross-border activity, face heightened exposure due to differences in compliance standards across jurisdictions. Furthermore, the speed with which financial instruments can be traded across multiple borders increases risks. The EBA Opinion on ML/TF risks also notes the sector's susceptibility to ML/TF threats arising from the anonymity and typologies associated with trading platforms, particularly in environments with limited oversight.

Vulnerabilities

The vulnerabilities of MiFID markets firms primarily stem from the nature of the trading platforms, which often facilitate high-speed trading and rely on an "execution-only" business model. This model means firms do not have insight into the rationale behind their customers' investment decisions, requiring robust controls to identify potentially suspicious behaviour. For example, customers may use rapid trading strategies or complex financial instruments to obscure the origin or purpose of transactions, while firms remain unaware of these underlying motivations. The SNRA highlights the risks posed by this lack of visibility, particularly in sectors like high-frequency trading, where transactional velocity and automation can present significant challenges for monitoring and oversight. The bilateral settlement of transactions occurs outside the trading venue as trading platforms do not hold customer assets or funds. This does mitigate the firm's risk vis-à-vis the non-movement of funds or assets. However, exposure to facilitation risk remains given the lifecycle of any particular transaction is not fully observable by the trading platform. The EBA Opinion on ML/TF risk impacting the EU financial sector underscores this point, noting that the incomplete view of transaction flows creates blind spots that could be exploited by bad actors performing illicit activities under the veil of complex trading strategies.

Control Weaknesses

The MiFID Markets firms sector demonstrates varying degrees of effectiveness in its AML/CFT systems and controls. While many firms have implemented adequate frameworks, there are areas in specific cases where controls could be further enhanced to be proportionate to a firm's inherent risk profile. Governance frameworks are an area for focus, with some firms unable to demonstrate sufficient oversight and that AML/CFT responsibilities are embedded at all levels. Similarly, risk assessment processes could be further enhanced to reflect the inherent complexity and cross-border nature of some firms' operations and commensurate mitigating controls could be implemented. Staff training presents another

area for improvement, with inconsistencies in the frequency and quality of AML/CFT training programmes. This limits firms' ability to adapt to dynamic ML/TF risks.

Strengthening governance oversight, improving the depth and relevance of risk assessments, and enhancing the rigour and regularity of employee training are key areas of focus for ensuring effective and consistent controls across the sector.

Retail Intermediaries

Risk Rating

	2019 Risk Ratings	2026 Risk Ratings
ML	Not Assessed	Low
TF	Not Assessed	Low
PF	Not Assessed	Low

Profile of Sector

Retail intermediaries encompass approximately 2,500 firms within Ireland which primarily deal with mortgage, general and life insurance, and investment products. However, only approximately 1,600 retail intermediaries who offer life insurance and/or investment products and services are designated persons under the CJA.[256]

Retail intermediaries range in size from large companies to sole traders. Traditionally, the majority are small-scale operations with low staff numbers with many operating as sole traders. However, this is changing with the emergence of some larger intermediary firms particularly in the insurance space. Clientele mainly consists of local and domestic customers, often introduced through existing relationships. Products offered typically originate from authorised entities such as investment and insurance firms. Retail intermediaries usually receive a fee or commission for having provided advice or assisted the customer in buying the product offered.

Threats

The primary ML threats in the retail intermediary sector arise from the potential misuse of life insurance or investment products, particularly those with features such as additional payment options or early surrender values. These features can make such products attractive for ML during the placement and layering stages, as they allow for the conversion of illicit funds into seemingly legitimate payouts. However, the ML threat level for this sector is assessed to be low, given that intermediaries act as distributors rather than controllers of the financial flows, with the responsibility for managing inherent ML risks sitting primarily with product providers.

[256] Retail intermediaries that only provide services in relation to mortgages and non-life insurance are not designated persons under the CJA.

Current threat intelligence does not suggest any significant TF or PF threats from the retail intermediary sector. The SNRA also notes that intermediaries operating within tightly regulated ecosystems, such as the insurance and investment markets in the EU, face relatively lower threats compared to sectors engaged in high-value or international financial transactions.

Vulnerabilities

The vulnerabilities faced by retail intermediaries are generally limited due to the nature of their role primarily acting as intermediaries between customers and regulated product providers. However, potential vulnerabilities still exist, particularly related to non-face-to-face sales processes. Transactions conducted remotely, such as online or over the phone, make it more difficult to verify the identity and intent of the customer, which creates opportunities for anonymity and misuse.

This non-face-to-face vulnerability is highlighted in the EBA Opinion on ML/TF risks, which emphasises the importance of strong CDD measures for remote interactions. Intermediaries may rely heavily on customer information provided directly by clients or third parties, which can obscure inconsistencies or red flags indicative of illicit activity. Furthermore, while retail intermediaries typically do not handle funds directly, their role as intermediaries means that weaknesses in customer identity verification or KYC processes could allow risks to flow upstream to product providers, impacting the resilience of the overall financial system.

Control Weaknesses

The retail intermediary sector generally has policies and procedures in place to meet AML/CFT obligations, but minor deficiencies persist in corporate governance and CDD. Smaller firms often lack formalised AML/CFT risk assessments and sufficient board oversight, meaning specific risks may not be effectively identified or mitigated. These weaknesses are partially mitigated by upstream providers, such as insurers and pension providers, who are required to conduct their own CDD on customers, reducing some vulnerabilities in intermediaries' frameworks. However, relying on such upstream controls creates gaps in the intermediaries' ability to monitor and manage their customer relationships independently. Strengthening governance, formalising risk assessments, and improving training for staff will be necessary to ensure a more consistent and robust approach to AML/CFT compliance across the sector.

High-Cost Credit Providers

Risk Rating

	2019 Risk Ratings	2026 Risk Ratings
ML	Not Assessed	Low
TF	Not Assessed	Low
PF	Not Assessed	Low

Profile of Sector

The High-Cost Credit Provider ("HCCP") sector in Ireland consists of 20 firms as of December 2025, collectively serving approximately 440,000 customers, with total assets amounting to €15 billion. The sector is characterised by a mix of firms, many of which are small-scale operations catering to specific customer needs, primarily within local or niche markets. Unlike other financial sectors with significant international exposure, all HCCPs operate exclusively within Ireland, providing an entirely domestic focus. These firms predominantly offer high-cost, short-term credit products to individuals, often targeting those who may face difficulties accessing traditional credit from banks or other institutions.

Threats

The HCCP sector in Ireland faces ML threats primarily related to its high reliance on cash transactions and the informal nature of its operations, which can make it vulnerable to misuse by criminal actors. Cash repayments provide opportunities for bad actors to integrate illicit funds into the financial system, particularly in smaller-scale laundering schemes. Additionally, the sector's customer base often includes individuals with limited access to mainstream financial services, a group that can be exploited by criminals to launder funds or facilitate financial flows on their behalf. The SNRA highlights that cash-intensive businesses, particularly those catering to underserved or financially vulnerable populations, are at heightened risk of being targeted by organised criminal groups. However, HCCPs are less likely to be used for high-value laundering schemes due to the typically small loan sizes and limited transaction volumes in the sector.

TF is considered a lesser threat within the HCCP sector due to the scale of activities and the domestic focus of firms. According to the EBA Opinion on ML/TF risks, smaller-scale financial

institutions with limited cross-border connections pose lower TF risks compared to internationally active sectors.

Vulnerabilities

The vulnerabilities in the HCCP sector largely stem from the limited scale and capacity of many firms and their reliance on more informal business models. Smaller firms often lack advanced compliance frameworks or sophisticated transaction monitoring systems, leaving gaps in their ability to detect structured repayments or unusual cashflows. The SNRA identifies these weaknesses as typical for cash-intensive businesses that rely on more direct customer interaction, especially where clear audit trails are difficult to establish. Additionally, many HCCPs operate without in-depth risk-based frameworks, relying instead on basic checks that may not adequately assess customer risks or sources of funds, thereby leaving the sector more susceptible to exploitation.

Furthermore, the domestic-only focus of the Irish HCCP sector, while limiting international exposure, does not fully eliminate risk. Vulnerabilities can arise from insufficient CDD, particularly when dealing with underserved populations who may have less formalised financial histories or verifiable documentation. The EBA Opinion on ML/TF risks flags non-face-to-face customer onboarding and limited use of technology for risk assessment as additional weaknesses, although likely only relevant to some firms in the sector.

Control Weaknesses

The HCCP sector demonstrates shortcomings across several key areas of AML/CFT compliance, despite the presence of basic frameworks. Engagements with the sector have identified a number of weaknesses, particularly with the documenting and tailoring of the firms' AML/CFT frameworks.

Deficiencies include weaknesses in the ML/TF risk assessments, where in some instances HCCPs had not undertaken such an assessment, or where the assessment was not sufficiently tailored to the HCCP's business model, limiting the firm's ability to implement an appropriate AML/CFT control framework. Similarly, AML/CFT policies and procedures are not always documented or tailored, which further limits a firm's ability to design and implement effective control measures.

Many HCCP firms are very small-scale operations with few employees, and as a result, their governance practices vary significantly from those of larger, more traditional lending institutions. This can lead to gaps in the documentation and oversight of policies, record-keeping, and monitoring systems, thereby hindering the detection of suspicious activity.

HCCPs have, in the past, been unable to demonstrate compliance with several obligations, including inadequate CDD, ongoing monitoring, and STR reporting. The absence of appropriate policies and procedures in these areas not only results in non-compliance by HCCPs but also increases their vulnerability to misuse for ML/TF activities.

Additionally, insufficient training programmes and a lack of robust screening and reporting mechanisms reduce the sector's effectiveness at identifying and escalating financial crime risks. Addressing these vulnerabilities will require stronger governance structures, clearer risk assessment methodologies, and enhanced training and monitoring processes to improve controls across the sector.

Non-Financial Services

Non-financial service providers in Ireland also represent a source of vulnerability to ML, TF, and PF, and many are designated as obliged entities under the CJA. The following sectors have been assessed:

- **Real Estate** – covering transactions involving land and property, including the activities of Property Service Providers and legal professionals.
- **Gambling Service Providers** – encompassing licensed betting offices, PMCs, and remote (online) gambling operators.
- **High Value Goods Dealers** – businesses accepting cash payments of €10,000 or more, including those dealing in luxury items such as vehicles, jewellery, and art.
- **TCSPs** – entities offering services related to company formation, directorships, nominee arrangements, and trust administration.
- **Legal Persons and Arrangements** – including certain partnerships and corporate structures that may be used to obscure beneficial ownership or facilitate illicit finance.
- **NPOs** – particularly those operating in high-risk jurisdictions or engaged in cross-border financial activities, where vulnerabilities to TF and PF may arise.
- **Legal Services Providers** – all other services outside of TCSP and conveyancing.
- **Accounting Services Providers** – all other services outside of TCSP.

These sectors are regulated by a range of authorities, including the PSRA, the AMLCU, and the Charities Regulator, depending on the nature of the entity and its activities.

Each sector was assessed using a consistent methodology that combines both qualitative and quantitative data to evaluate exposure to ML, TF, and PF risks. Sources included regulatory reports, supervisory assessments, publicly available data, and insights from law enforcement, Government bodies, industry stakeholders, and individual firms. International publications, such as those from the FATF and the EU SNRA, were also considered to ensure alignment with global practice.

To supplement these data sources, sector-specific surveys were issued to gather additional insights directly from industry participants, on a voluntary basis. These surveys focused on the structure and activities of entities, perceptions of ML, TF, and PF risks, and the internal controls in place to mitigate those risks. While the surveys provided valuable context and helped form a picture of the industry perspective, low response rates in some sectors limits to some extent the ability to draw firm conclusions about sectors' risk exposure.

Table 21: Response rate breakdown across DNFBP groups

Sector	Group	Responses	Recipients	Response Rate
Gambling Service Providers	PMCs	8	11	73%
HVGDs	Motor Industry	82	1,260	6%
TCSPs	TCSP Firms	249	1,287	19%
Non-Profit Organisations (''NPOs'')	CRA Regulated Charities	1,425	9,273	15%

Real Estate

Executive Summary

	2019 Risk Ratings	2026 Risk Ratings
Real Estate Assets		
ML	Not Assessed	Significant
TF	Not Assessed	Moderate
PF	Not Assessed	Low
Property Service Providers		
ML	Medium-Low	Moderate
TF	Medium-Low	Moderate
PF	Not Assessed	Low
Legal Services		
ML	Medium – High*	Significant
TF	Medium – High*	Moderate
PF	Not Assessed	Low

**The ML/TF risk rating assigned in 2019 took into account all relevant services which bring solicitors and barristers within the scope of the CJA. The 2025 risk assessment assesses risks solely as they are associated with conveyancing services.*

Key Insights

From a ML perspective, real estate assets can be used both as a means to launder and integrate funds and as a final asset for wealth accumulation by criminals and OCGs. Although there are opportunities for TF in the real estate sector (and as noted in the EU SNRA, these are similar in nature to the ML risks), there have been no TF prosecutions or court cases with a nexus to Ireland.

The key vulnerabilities within the sector are:

- **Intentional or unintentional failure to apply risk-based due diligence:** Third parties such as solicitors and Property Service Providers play a critical role in applying risk-based due diligence in real estate transactions. Given the high values involved in real estate transactions, failures to apply these processes can create significant vulnerabilities to ML/TF/PF activities.

- **Ownership structures:** The use of complex ownership structures in real estate, especially those involving high-risk jurisdictions, offshore entities, or even seemingly simple arrangements such as those involving family members, can obscure beneficial ownership and heighten ML/TF risks.

- **Direct property sales outside regulatory oversight:** Direct sales by property developers, builders, and vendors may fall outside of the regulatory environment; in addition, transactions that do not require the use of a mortgage or other credit product will be subject to lesser due diligence.

- **Illicit foreign investment in Irish real estate:** Law enforcement has identified instances where Irish property has been purchased by foreign buyers, using suspected criminal funds.

Legislative and Regulatory Framework for the Real Estate Sector

Property Service Providers and solicitor (as defined below) firms in Ireland are 'designated persons' under the CJA. All firms in the sector are subject to supervision in relation to their AML/CFT frameworks. In addition to the CJA, solicitors are subject to the Solicitors (Money Laundering and Terrorist Financing Regulations) 2020, and solicitors are also required to comply with the requirements of the Solicitors Accounts Regulations 2023, which outlines requirements for the protection of client monies held by solicitors.

Defining the Real Estate Sector

In assessing the real estate sector in Ireland, the following sub-sectors have been considered in respect of their risk profile and associated vulnerabilities to ML, TF, and PF:

1. **Real Estate Assets:** refers to land and anything permanently affixed to it, such as buildings and structures;

2. **Property Service Providers:**[257] persons who by way of business carry out any of the following services in respect of property located in or outside the State:

    - Persons involved in the auction of goods and chattels;[258]
    - Persons involved in the purchase/sale of real estate;
    - The letting of real estate;
    - Property management services.

[257] As defined in the Property Service (Regulation) Act 2011 and the CJA 2010, Section 24
[258] For detailed discussion of this cohort see the chapter on High Value Goods Dealers

3. **Legal Services Providers:** engaging the use of a solicitor for conveyancing services (i.e. "services in connection with the preparation of transfers, conveyances, contracts, leases or other assurances in connection with the disposition or acquisition of estates or interests in land").[259] Also includes the use of public notaries in respect of real estate transactions.

In addition, financial institutions (including banks) play a key role in facilitating the payments necessary to complete real estate transactions. These institutions are assessed in the financial services sectoral risk assessments.

Scale and Structure of the Real Estate Sector in Ireland

There are 2.1 million[260] permanent dwellings in Ireland, and 60,300 residential property transactions were completed in 2024, with a combined value of over €26.2 billion.[261] Of these, 139 transactions were conducted with values in excess of €5 million, 68 of which were for amounts exceeding €10 million. In addition, Irish commercial real estate is valued at €144 billion as of June 2024.[262] There is concentration in investment in Irish commercial real estate, looking at figures for 2022 and 2023, the top 10 investors accounted for 70% of total investment. A "meaningful proportion" of commercial real estate assets are likely held by, or funded by, overseas entities on a cross-border basis.[263]

At the end of 2024, there were 5,952 property service provider licensees in Ireland. These consist of 1,814 licensed businesses (e.g. employers) and 4,138 individuals licensed to carry out property services.[264] There were 12,683[265] registered practising solicitors in Ireland as of February 2025, and 2,443 law firms.

[259] Solicitors (Amendment) Act, 1994, Section 56 Paragraph 4
[260] Central Statistics Office / Census of Population 2022 / Available from: https://www.cso.ie/en/statistics/population/censusofpopulation2022/
[261] Residential Property Price Register - Property Services Regulatory Authority / Available from: https://www.propertypriceregister.ie/Website/NPSRA/pprweb.nsf/page/ppr-home-en
[262] Central Bank of Ireland / Financial Stability Review 2024 / Available from: https://www.centralbank.ie/docs/librariesprovider2/financial-stability-review/financial-stability-review-special-feature-commercial-real-estate---a-macro-financial-assessment.pdf / p.5
[263] Ibid. / p.4
[264] Property Services Regulatory Authority / Annual Report 2024 / Available from: https://www.psr.ie/wp-content/uploads/2025/06/PSRA-Annual-Report-2024-Final-English.pdf / p.20
[265] Law Society of Ireland data

Real Estate Assets

The Irish real estate market is attractive for ML due to sustained price appreciation, the high value of funds involved, and its appeal as a lifestyle asset for criminals. Criminals use real estate both as part of laundering schemes and as a final destination for illicit funds.

Real estate can be used in multiple ways in ML, TF, and PF schemes, including:

- Manipulation of appraisal or valuation of real estate to enable movement of value between parties;
- Purchasing the property with illicit funds and holding the property either to live in, or to generate a seemingly legitimate rental income;
- Buying the property with illicit funds, and re-selling the property to launder the funds (noting that while this approach of cleaning funds is slower than other approaches, the large values and relative ease of access to the sector makes it more attractive than it otherwise would be);
- Use of simple or complex ownership structures, including arrangements involving family members, or other opaque mechanisms to conceal beneficial ownership;
- Investing of illicit funds to renovate real estate assets and to benefit from the increased value of the asset;

Section 2(1) of the Proceeds of Crime Act[266] allows CAB to make orders against property which constitutes the proceeds of crime. In 2024, orders were made against 4 real estate assets (valued at €1.4 million), down from 21 in 2023.[267]

Table 22: Real Estate Assets over which orders were made[268] and value of assets frozen[269] (2020 – 2024)

Sector	2020	2021	2022	2023	2024
Value of Real Estate Frozen	€3,798,716	€954,178	€1,270,144	€5,277,635	€1,421,295
Orders against Real Estate	19	7	12	21	4

[266] Proceeds of Crime Act 1996 / https://revisedacts.lawreform.ie/eli/1996/act/30/revised/en/pdf?annotations=false
[267] Criminal Assets Bureau / Annual Report / Available from: https://www.cab.ie/wp-content/uploads/2024/10/CAB-Annual-Report-2024-Final.pdf / p.34
[268] Assets over which section 2(1) orders were made under the Proceeds of Crime Act 1996 to 2016
[269] Assets frozen under section 2 of the Proceeds of crime act 1996 to 2016

Property Service Providers

Property Service Providers are engaged by the vendor, and facilitate the sale of real estate assets. The PSRA is the statutory body with responsibility for licensing and regulating the Property Service Providers (including auctioneers and estate agents) in Ireland. Property Service Providers are designated persons under the CJA, and are therefore required to conduct activities such as risk-based due diligence, the reporting of suspicious activity, etc.

Although it is not prohibited, Property Service Providers generally do not accept cash deposits and instead process transactions through client accounts held with financial institutions. In addition, where cash is accepted and is €500 or greater, a cash origin form is generally completed in order to identify the source of the funds. Transactional activity will therefore be subject to monitoring by those financial institutions. In its role as competent authority, the PSRA conducts AML/CFT reviews of all licensed firms at least every five years, and all newly licensed businesses are reviewed within a two year period after authorisation.

While most property transactions in Ireland involve regulated Property Service Providers, there is no data confirming the extent of sales conducted without the use of a Property Service Provider. Certain types of transactions – including those conducted directly by developers, builders or private individuals – can occur without the use of a Property Service Provider and may therefore not be subject to the same levels of vendor/purchaser due diligence.

Legal Services Providers

Solicitors play a key role in the transaction of selling and purchasing a property, as they are engaged in most instances by both the purchaser and vendor to provide legal advice in relation to the sale and purchase; this process is known as conveyancing.

Solicitors are designated persons in the CJA, and are supervised from an AML/CFT perspective by the Law Society of Ireland,[270] and are therefore subject to AML/CFT requirements, including the requirement to conduct risk-based due diligence (including source of funds checks on the buyer), report suspicious activity, etc.

Solicitors are engaged by both the purchaser and vendor to complete conveyancing services, and will generally receive and transfer large fund values necessary to complete the transaction. This process includes transfers into a client money account held by the

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

purchaser's solicitor, from the purchaser and, where applicable, mortgage providers. These funds are then disbursed to the vendor's solicitor's accounts and subsequently to vendors. Discussions with firms in the sector, and the Law Society, indicate that while the use of physical cash in real estate transactions is not prohibited, it is highly uncommon. In most cases, the presence of multiple third parties – including solicitors, Property Service Providers, and the financial institutions (including those providing services to the buyer, the vendor, and the solicitors) – all of which are subject to the CJA, creates multiple opportunities within the process to identify and report suspicious activity.

Threats and Vulnerabilities

Threats

The ML, TF, and PF threats to which Ireland is exposed are assessed above. The real estate sector is exposed to a broad range of threats, in particular fraud, sanction evasion, proceeds of drug offences, and illicit foreign investment. The sector facilitates the acquisition and transfer of high-value assets, involving complex or layered ownership structures, which can be exploited to launder proceeds of crime or obscure the origin and control of funds. Fraudulent funds, including those derived from investment scams or property-related deception, may be used to purchase real estate as a method of integrating criminal proceeds into the legitimate economy. Drug trafficking networks also look to use real estate to store or convert illicit gains. Illicit foreign investment, especially where beneficial ownership is obscured or funds originate from high-risk jurisdictions, presents elevated risks.

Despite the large number of practising solicitors (12,683), law firms (2,443), and licensed Property Service Providers (5,952), registration with FIU Ireland is low, only 312 solicitors and 164 Property Service Providers are currently registered to submit STRs. In 2024, these sectors submitted just 30 STRs, of which 13 related to property purchases or rentals. Of these, 10 have been fully analysed resulting in 4 disseminations, 3 to law enforcement and 1 to other FIUs. All STRs submitted cited ML. The low level of reporting and the known level of criminal activity may highlight gaps in STR reporting, within the legal and property sector.[271]

[271] Not all practising solicitors provide AML- regulated legal services and some law firms elect to register only their Money Laundering Reporting Officer to submit STR reports on behalf of all solicitors in their firm who provide AML- regulated legal services.

Vulnerabilities

In assessing the vulnerabilities of the real estate sector in Ireland to ML, TF, and PF threats, this risk assessment has considered FATF[272] guidance and the results of the EU Supranational Risk Assessment. The scale, structure and nature of the real estate sector in Ireland has also been assessed, including the extent to which the sector has implemented proportionate controls to mitigate the identified threats.

Vulnerability 1: Intentional or Unintentional Failure to Apply Risk-Based Due Diligence

Given the large volume and value of real estate transactions, and the key role played by third parties (such as Property Service Providers, solicitors and valuers) in mitigating ML, TF, and PF risks, failures to apply adequate due diligence can open the market to abuse. In particular, solicitors are central in ensuring appropriate due diligence – including checks relevant to source of funds, and beneficial ownership of legal persons being used to purchase real estate – is conducted. Failures to apply due diligence could be unintentional, for example due to a lack of understanding or capacity among third parties, or intentional: i.e. where the third-party is knowingly involved in the ML, TF or PF operation, including as part of professional ML operations linked to OCGs, or potentially for their own personal gain.

Case Study: Real Estate Fraud and the Role of Professional Gatekeepers

This case involves fraudulent property registrations and the laundering of proceeds through professional intermediaries. The scheme included the dishonest appropriation of €21,875 in rent and €246,250 in lease buy-out funds, with attempts to conceal and transfer these funds both domestically and internationally.

Solicitor's Role: A solicitor facilitated the fraudulent registration of property titles by improperly transferring ownership through the Property Registration Authority for two properties.

Accountant's Role: An accountant assisted in laundering the stolen funds by moving €21,875 in rent and €246,250 in lease buy-out money through various accounts, including attempts to transfer funds to bank accounts in the USA.

[272] FATF / Guidance for a Risk-Based Approach / Available from: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/RBA-Real-Estate-Sector.pdf.coredownload.pdf

The Law Society plays a role in mitigating this risk through its regulatory oversight, conducting approximately 350 inspections per year, including reviewing the AML/CFT frameworks in place in its regulated firms. These inspections are conducted as assessments of a range of related risk areas, including the framework for protecting client funds in line with the Solicitors Accounts Regulations.[273] Between January 2023 and June 2024, the Law Society of Ireland issued directions which required three solicitors' practices to be subject to external audits[274] and referred three solicitors to the Legal Practitioners Disciplinary Tribunal due to AML compliance failures noted during inspections.

The PSRA also conducts reviews of Property Service Providers' compliance with CJA requirements, and over the last four years areas of non-compliance were identified in 11% of AML audits carried out.[275] These cases resulted in PSRA interventions, which in all cases resulted in Property Service Providers submitting evidence of enhanced compliance standards. The most common breaches related to ML/TF Business Risk Assessments, Customer Risk Assessments and CDD. Whilst the PSRA is the competent authority for Property Service Providers compliance with the CJA, it lacks enforcement powers (e.g. licence revocations) to sanction Property Service Providers for AML/CFT failures, which limits both the effectiveness of findings issued by the PSRA and reduces persuasive powers to implement effective ML, TF, and PF controls. In its July 2024 report[276] assessing technical compliance, the FATF noted that Ireland scored above the FATF average in technical compliance standards as they apply to gatekeepers, including lawyers and notaries and Real Estate Agents.

Vulnerability 2: Complex or Opaque Ownership Structures

Complex ownership structures can be used to purchase real estate in Ireland, which can inhibit the identification of the beneficial ownership of the asset. These complex ownership arrangements, particularly when linked to high-risk jurisdictions or offshore entities, can pose heightened risks.

Law enforcement has also identified cases in which criminal owned properties have been registered in the name of the construction company. This arrangement could have been established either with or without the knowledge of the construction company; however,

[273] S.I. No. 118/2023 - Solicitors Accounts Regulations 2023
[274] Law Society of Ireland / Annual Report and Accounts 2023/2024 / Available from: https://www.lawsociety.ie/globalassets/documents/about-us/annual-reports/23-24/annual-report-2024-full.pdf / p.63
[275] Property Services Regulatory Authority / Annual Report 2024 / Available from: https://www.psr.ie/wp-content/uploads/2025/06/PSRA-Annual-Report-2024-Final-English.pdf / p.35
[276] FATF / Horizontal Review of Gatekeepers' Technical Compliance Related to Corruption / Available from: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/HRGTC.pdf.coredownload.inline.pdf / p.13

construction and real estate industries have been noted as one of the sectors particularly affected by criminal abuse.[277]

Case Study: Real Estate and Organised Crime

A Dublin based convicted drug dealer linked to OCGs used illicit funds to purchase multiple properties. The High Court accepted that his main income was from drug dealing, and the individual could not explain how he legitimately financed the properties. The properties included a €1.7 million property in the southeast of the country, funded through six different transfers using four different individuals.

The individual was shown to be in receipt of social welfare and pandemic unemployment payments without declaring rental income received from the property portfolio. In April 2024, the High Court ordered the confiscation of the properties, ruling they were bought with criminal proceeds.

Vulnerability 3: Direct Property Sales Outside Regulatory Oversight

While property transactions are mostly conducted through Property Service Providers subject to the CJA, property developers, builders and vendors can also sell properties directly to buyers without using regulated Property Service Providers; these sales are not subject to the same level of scrutiny. In addition, some property transactions are financed without the need for a mortgage.

The following transaction types present heightened risks:

- Purchasing property without a mortgage removes lender oversight, removing independent source of funds checks by a regulated financial institution.
- Purchasing property without an estate agent eliminates a layer of professional scrutiny.
- Purchasing property without a buyer-side solicitor removes essential legal safeguards, and even where a solicitor is involved, if they are compromised or operating in a jurisdiction with weak regulatory oversight, they may be actively facilitating criminal operations.

[277] Europol / The changing DNA of serious and organised crime / Available from: https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf / p.27

Vulnerability 4: Illicit Foreign Investment in Irish Real Estate

Law enforcement has identified instances where Irish property has been purchased by foreign buyers, using suspected criminal funds. The Irish property market is attractive to illicit international finance for similar reasons as it is for legitimate buyers, in that Irish real estate assets have tended to maintain or appreciate in value in recent years, and that Ireland benefits from stable rule of law.

This issue is not isolated to Ireland, as countries with similar open economies have identified the same concerns. Specifically, the London real estate market – in particular premium real estate assets – has been targeted for investment by HNWIs with questionable source of funds from Russia and other jurisdictions. This has included properties linked to sanctioned individuals[278] being bought and held through complex legal ownership structures. Canada has also identified similar concerns and has subsequently extended its ban on foreign ownership of residential properties.[279] Similar restrictions on foreign ownership of real estate are in place in other jurisdictions, including Switzerland, Denmark and New Zealand.

Red Flags for illicit overseas investment into Irish real estate

As noted by law enforcement, there has been an increase in the level of investment into Irish real estate from international buyers, often from China. Common indicators of suspicion in relation to these transactions include:

- The buyer appears to have no legitimate source of income and/or there is no explanation as to the source of funds for the property, particularly if they are attempting to purchase a high value property.
- Property is being bought through a legal entity, including a Trust.
- Funds being sent directly from an overseas bank account to the solicitor's account (i.e. not via an Irish bank account).
- The individual buying the property is not the individual who is being listed as the beneficial owner of the property.

[278] Transparency International UK / The enablers within: how UK professionals are helping Russian elites evade asset freezes / https://www.transparency.org.uk/news/enablers-within-how-uk-professionals-are-helping-russian-elites-evade-asset-freezes
[279] Government of Canada / Government announces two-year extension to ban on foreign ownership of Canadian housing / https://www.canada.ca/en/department-finance/news/2024/02/government-announces-two-year-extension-to-ban-on-foreign-ownership-of-canadian-housing.html (note, this action was also taken to address housing affordability)

Consequence

A substantive ML, TF or PF incident in the real estate sector would cause serious harm to the integrity of the sector and could have far reaching consequences for related sectors, including banking, legal services and property service providers. Given the vital role of the property sector in Irish society, and its exposure to international investment, such an incident would impact Ireland's international reputation. As such, consequence has been rated as very significant.

EU Supranational Risk Assessment

The EU Supranational Risk Assessment assessed the real estate sector in its most recent (2022) risk assessment as per the below:

TF Risk	ML Risk
Very Significant	Very Significant

The risk factors identified within this sectoral risk assessment are aligned with those set out in the EU Supranational Risk Assessment.

Horizon Scanning

International Developments in Restrictions on Foreign Ownership

As noted, several countries have taken action to restrict or ban foreign ownership of residential real estate assets. Should additional countries take similar steps (with Ireland declining to), this could lead to Irish real estate becoming increasingly attractive for both legitimate and illegitimate investments.

Single Access Point to Real Estate Information

AMLD6, published in 2024, requires Member States to establish a single electronic access point through which competent authorities and AMLA can obtain immediate, direct, and free access to comprehensive real estate data. This includes property details, ownership information, encumbrances, history of property ownership and price, and relevant supporting documents.

Gambling Service Providers

Executive Summary

	2018/2019 Risk Ratings*	2026 Risk Ratings
Retail Bookmakers		
ML	Medium-Low	Moderate
TF	Medium-Low	Low
PF	Not Assessed	Low
On-course Bookmakers		
ML	Medium-Low	Moderate
TF	Medium-Low	Low
PF	Not Assessed	Low
Remote Bookmakers (Betting Intermediaries and Exchanges)		
ML	Medium-Low	Significant
TF	Medium-Low	Low
PF	Not Assessed	Low
Private Members' Clubs (PMC)		
ML	Medium-High	Significant
TF	Medium-High	Low
PF	Not Assessed	Low
Lotteries and Bingo Operators**		
ML	Low/Medium-Low	Moderate
TF	Not Assessed	Moderate
PF	Not Assessed	Low
The Tote (both Horse Racing Ireland ("HRI") and Greyhound Racing Ireland ("GRI")		
ML	Medium-Low	Low
TF	Medium-Low	Low
PF	Not Assessed	Low

**The gambling industry was assessed in 2018, excluding PMCs. However, PMCs were evaluated in the 2019 NRA, and the relevant ratings have been assigned accordingly.*

***The National Lottery and Bingo Operators are assessed as being low risk for ML, TF, and PF.*

Key Insights

The gambling and related sector in Ireland comprises of a number of distinct activities and different types of businesses posing varying degrees of ML, TF, and PF risks. From a ML perspective, gambling can be used both as a means to launder funds, as well as being used as an end product for illicit gains (lifestyle choice) by criminals.

The key vulnerabilities within the sector are as follows:

- **Cash-Intensive Nature:** The gambling sector is highly cash-intensive, although there is a shift to online activity. Cash-based gambling activity can make it difficult to trace the source of funds, monitor aggregate spend, and identify suspicious activity. Cash transactions are inherently less transparent and more susceptible to ML and, to a lesser extent, TF and PF.

- **Potential for Criminal Ownership or Influence:** The cash-intensive nature of physical gambling premises increases the risk of criminal or OCG ownership or influence, as high volumes of untraceable cash transactions make these venues attractive for laundering illicit funds and enable employee collusion or coercion. In contrast, online platforms face heightened risks due to the sheer scale of digital transactions, which can facilitate large-scale ML.

- **Difficulties in Customer Identification:** Customer identification is a persistent challenge across the gambling sector, especially at physical premises. The cash-based nature of these environments, increasing the risk of anonymous transactions and complicating efforts to detect ML.

- **Use of Gambling as a Lifestyle Choice:** Criminals engage in gambling not just to launder funds but as a lifestyle choice, integrating illicit funds into the legitimate economy through regular gambling activity.

The gambling sector assessment highlights inherent vulnerabilities that could make it susceptible to ML and TF. However, in practice, the primary ML threats tend to arise from gambling being used as a lifestyle choice or as a means of cash-washing. The overall risk of placement across the industry remains relatively low, which limits the scale and complexity of laundering activities observed in practice.

Legislative and Regulatory Framework for Gambling Industry

'Gambling services' means "a service which involves wagering a stake with monetary value in games of chance, including those with an element of skill such as lotteries, casino games, poker games and betting transactions that are provided at a physical location, or by any means at a distance, by electronic means or any other technology for facilitating communication, and at the individual request of a recipient of services".

In an Irish context, games of poker played outside casinos or PMCs, lotteries as defined by the Gaming and Lotteries Act 1956, and gaming machines are not considered gambling services.

Under the CJA, gambling service providers are classified as “designated persons”, and are therefore subject to its requirements.

While the CJA governs AML obligations, the general regulatory framework for gambling in Ireland is undergoing significant reform. As noted in Table 23 below, the current licensing and supervisory framework for the gambling industry is spread across multiple agencies. However, the Gambling Regulation Act 2024 aims to modernise and consolidate gambling regulation in Ireland, and will establish the GRAI as the competent authority. Until it becomes fully operational and the GRAI is adequately resourced, the AMLCU at the Department of Justice will remain the designated competent authority for the sector.

A new comprehensive gambling licensing regime will be introduced for gambling activities, which includes betting, gaming and lottery activities, as well as the sale or supply of gambling products or related gambling services. The licensing framework is being prepared with public consultations and draft regulations. Licences will be granted subject to funding winnings by lawful activities, which is a key AML/CFT prevention measure.

The GRAI has granted wide-ranging sanction and enforcement powers under Part 8 of the Gambling Regulation Act 2024, including the power to issue a compliance notice; direct an investigation; apply to court for suspension or revocation of a licence or to block access to online services; conduct an oral hearing; apply for emergency orders to protect the public from serious consequences of an ongoing contravention, including blocking access to online services; and impose administrative sanctions including financial penalties (up to €20,000,000 or, if greater, 10% of the licensee’s turnover) or the suspension, revocation or imposition of a condition on any gambling licence.

Scale and Structure of the Gambling Sector in Ireland

Table 23: Breakdown of the sub-sectors within the gambling industry in Ireland

Type	Description	Total # Licenses Issued	Annual revenue generated	Regulatory Framework[280]
Retail Bookmakers	Physical betting shops offering gambling services	753	2023 - €2,403.1 million[281]	Licensing: Revenue Commissioners Supervisor: AMLCU (Department of Justice)
On-course Bookmakers	Operate at racecourses, offering betting services directly to attendees	166	2023 – €71.7 million[282]	Licensing: Revenue Commissioners Supervisor: AMLCU (Department of Justice) and HRI
Remote Bookmakers Bookmakers & intermediaries	Online platform offering gambling services	93	2023 - €2,561 million[283]	Licensing: Revenue Commissioners Supervisor: AMLCU (Department of Justice)
Private Members' Clubs	Clubs offering gambling services to members	12	Not available	Licensing: District court Supervisor: AMLCU (Department of Justice)
National Lottery	Funds public good causes and offers games like Lotto and EuroMillions.	Lottery - 5,175 Bingo – 970	2023 – €829.4 million[284]	Licensing: Regulator of the National Lottery Regulator: Regulator of the National Lottery

[280] The Gambling Regulation Act 2024 established the Gambling Regulatory Authority of Ireland (GRAI) as the competent authority for licensing and supervision, except for the National Lottery, which will retain its dedicated regulator.
[281] Revenue / Betting Duties / Available from: https://www.revenue.ie/en/corporate/information-about-revenue/statistics/excise/betting-duty/index.aspx
[282] Horse Racing Ireland / Factbook 2023 / Available from: https://www.hri.ie/HRI/media/HRI/Comms/Documents/HRI-Factbook-2023_FINAL_interactive.pdf / p.6
[283] Revenue / Betting Duties / Available from: https://www.revenue.ie/en/corporate/information-about-revenue/statistics/excise/betting-duty/index.aspx
[284] Regulator of the National Lottery / Annual Report 2023 / Available from: https://www.rnl.ie/assets/PDFs/annual-reports/Regulator-AR-2023-English.pdf / p.7

Local Lotteries	Lotteries authorised by the courts for charitable or community purposes. Permits are issued by An Garda Síochána for lotteries under €10,000 and District Courts for lotteries above.	Not available	Not available	Licensing: District court and An Garda Síochána Oversight: An Garda Síochána
Tote betting providers	Pool betting services, associated with horse and greyhound racing	2	HRI 2023 - €71.2 million[285] GRI 2023 - €15.2 million[286]	Licensing: Dept of Finance, upon request from the Minister of Agriculture Supervisor: HRI/GRI

Scale and Structure of the Betting Sector in Ireland

Betting, which involves placing a wager on the outcome of an event, is regulated by the Betting Act 1931[287] (as amended). In Ireland, betting operators include:

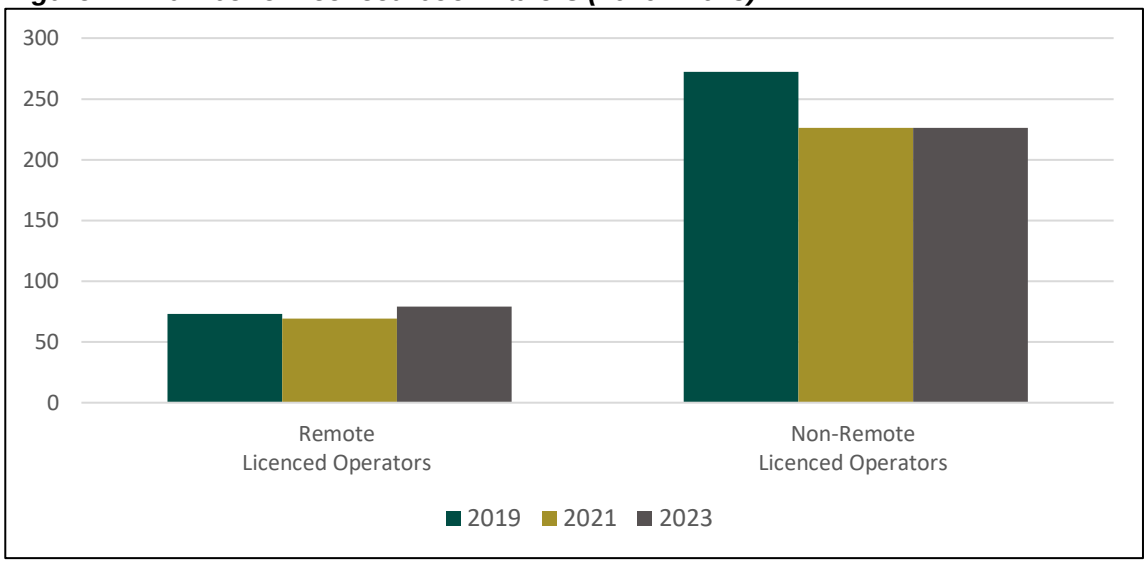
- Retail bookmakers (non-remote)
- On-course bookmakers (non-remote)
- Online bookmakers and betting intermediaries (remote)

A bookmaker is defined as "*a person who, in the course of business, takes bets, sets odds and undertakes to pay out on winning bets*". [288]

[285] Horse Racing Ireland / Factbook 2023 / p.6
[286] Greyhound Racing Ireland / Annual Report 2023 / Available from: https://www.grireland.ie/globalassets/report-pdfs/annual-reports/rce-2023-annual-report.pdf / p.9
[287] Electronic Irish Statute Book (eISB), Acts of the Oireachtas, Betting Act, 1931.
[288] Revenue / Bookmaker's Licence / Available from: https://www.revenue.ie/en/companies-and-charities/excise-and-licences/excise-licensing/bookmakers-licence/index.aspx

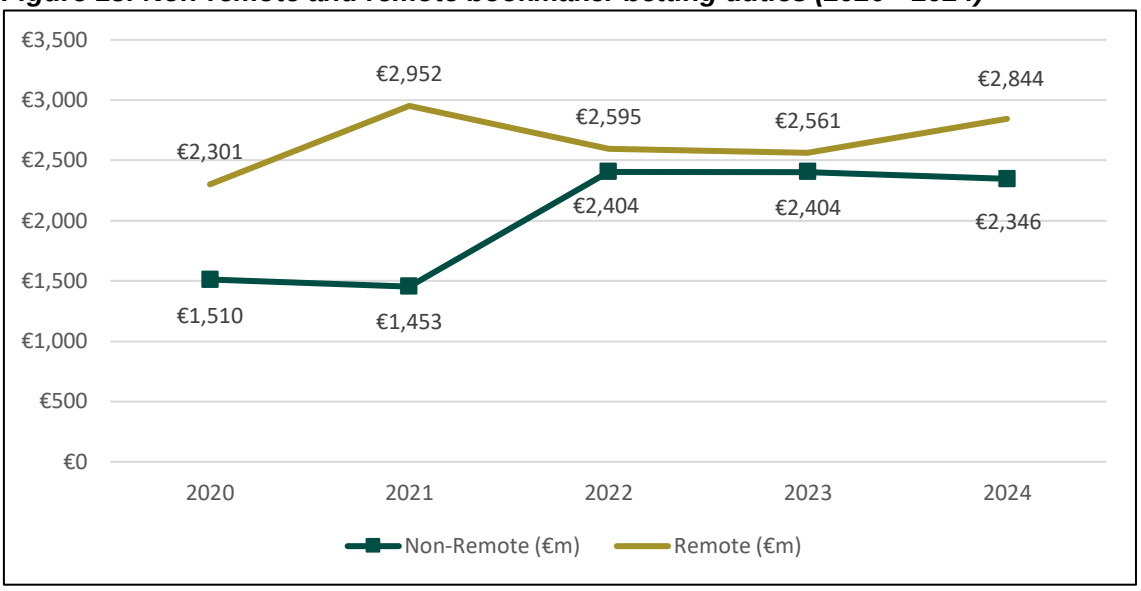
Revenue requires all relevant officers of Bookmaker's Licence applicants to hold a Certificate of Personal Fitness from An Garda Síochána (Irish entities) or the Department of Justice (non-Irish domiciled entities). Licences are non-transferable, and a new certificate is needed for changes in ownership.

Figure 12: Number of licenced bookmakers (2019 - 2023)[289]



[289] As per submissions by Revenue, Registers for Bookmakers, premises and licences. Note: licences are issued every two years.

Figure 13: Non-remote and remote bookmaker betting duties (2020 - 2024)[290]



Threats and Vulnerabilities

Threats

The ML, TF, and PF threats to which Ireland is exposed are assessed above. Within this context, the gambling services sector is primarily exposed to direct ML risks, particularly in relation to predicate offences that generate large volumes of cash. Criminals and OCGs exploit the sector's capacity to accept and circulate cash, using it as a vehicle for cash-based ML. Gambling services may also be used as a lifestyle choice by criminals to integrate illicit funds into the legitimate economy. Where control frameworks are weak, particularly in online gambling environments, these platforms may be exploited to move funds and introduce them into the financial system with reduced traceability.

As of May 2025, a total of 60 gambling service providers are registered with FIU Ireland. These entities are not categorised by specific types, and therefore, a detailed breakdown by type is currently unavailable. In 2024, gambling service providers submitted 454 STRs to FIU Ireland. Of these, 331 reports have been fully analysed, resulting in 117 disseminations, 110 to law enforcement agencies and 7 to foreign FIUs, representing 33.5% of the analysed reports. The remaining 123 STRs are still under review by FIU Ireland. Of the total STRs

[290] Revenue / Bookmaker's Licence / Available from: https://www.revenue.ie/en/companies-and-charities/excise-and-licences/excise-licensing/bookmakers-licence/index.aspx

submitted, 99% were classified by reporting entities as related to ML, while fewer than 1% were associated with TF.

Retail Bookmakers (non-remote)

Risk Rating

Retail bookmakers are assessed as posing a moderate risk for ML, and a low risk for TF and PF. This moderate ML risk stems from their cash-intensive operations and the presence of multiple premises and operators, which can hinder the detection of suspicious activity. This is mitigated in large part by the use of closed-loop systems[291] for payouts, which limit opportunities for misuse, including for TF and PF.

Overview of Retail Bookmakers

Retail bookmakers consist of physical bookmaking premises, including both independent operators and the non-remote elements of the large corporate bookmaking entities. The number of retail betting shops in Ireland has declined by 43% in recent years,[292] going from 1,385 premises in 2008 to 787 in 2023, which has coincided with a move towards online betting and consolidation of operators in the market. The Irish retail bookmaking industry is largely controlled by three gambling service providers, which between them account for 84% of retail bookmaking premises.[293]

The risk landscape varies between independent operators and the large operators in the sector. Independent bookmakers generally have a lower customer footfall and a more regular customer base, and large bets from non-regulars would likely be more apparent and treated with greater suspicion. Large-scale entities are inherently more exposed to ML risks, as they have multiple premises, which provides scope for customers to place bets in different outlets. However, they are also more likely to apply more mature, and technology enabled mitigating controls, such as automated monitoring systems and dedicated ML and TF compliance and risk resources.

Vulnerability 1: Cash-Intensive Nature

[291] A payment setup where funds stay within the same verified account (e.g., the customer's betting account), preventing transfers to third parties or external instruments.
[292] Irish Bookmakers Association Report
[293] Revenue data

The cash-intensive nature of retail bookmakers makes them susceptible to ML activities. The high value and volume of cash receipts make it challenging to identify and verify source of funds, monitor transactions and conduct effective oversight. The difficulty in tracking aggregate spend for cash transactions to trigger CDD, as required by the CJA,[294] hinders the identification of suspicious activities and complicates the implementation of robust AML measures.

Vulnerability 2: Accessibility to Multiple Premises and/or Operators

Individuals can exploit the fact that they can bet in multiple retail premises with different operators, making it challenging to monitor transactions and identify suspicious activity. The placing of bets across multiple premises or operators allows individuals to disguise betting patterns and inhibits the ability of gambling operators to identify linked transactions and/or perform effective due diligence and ongoing monitoring.

Vulnerability 3: Features of Betting Products

The transferable nature of betting receipts allows bets to be placed and collected by different individuals – even where funds are ultimately attributed to a single beneficiary. This inhibits the ability of gambling operators to link transactional activity and identify suspicion. The fixed odds nature of the products enables structured or minimal loss betting strategies; these can be difficult to identify, as legitimate customers may employ similar tactics. Self-service betting terminals, widely used by large corporate betting operators, make it challenging to identify customers, as there is no direct interaction between the customer and staff.

Vulnerability 4: Collusion and Criminal Influence

Betting operations are exposed to the risk of being acquired or influenced by criminals or OCGs to launder criminal proceeds. Additionally, bookmaker employees may collude with criminals or be intimidated by known criminals to facilitate laundering or the acceptance of funds where there is suspicion of ML.

[294] Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 / Responsibilities of Designated Persons, Section 33.

On-course Bookmakers

Risk Rating

On-course bookmakers are assessed as posing a moderate risk for ML and a low risk for TF and PF. While they share similar vulnerabilities with retail bookmakers such as cash-based transactions and challenges in identifying suspicious activity, their smaller scale and operating environment make them less attractive for ML. The practice of returning winnings via cash or verified bank accounts helps limit opportunities for ML and TF, though it does not fully mitigate risks such as cash washing or the use of criminal funds in gambling as a lifestyle choice.

Overview of on-course Bookmakers

In 2024, there were 390 horse racing meetings in Ireland, with a total attendance above 1.2 million. On-course betting in 2024 amounted to €75 million,[295] with average wagers ranging between €15 and €20.[296] HRI is the regulatory body for bookmakers and betting in the horse racing industry, although their primary focus from a regulatory standpoint is maintaining integrity in the sport, rather than specifically on AML/CFT. All on-course bookmakers must obtain a permit from the HRI which has the power to suspend or revoke permits, and HRI inspectors attend every meeting to supervise bookmaking activity.

There are 166 on-course bookmakers across Ireland.[297] On-course bookmakers have limited exposure to ML in terms of placement, as winnings are paid out in cash and betting receipts are retained by the bookmaker. However, the cash-based nature of operations can still facilitate cash-washing. That said, the opportunity to execute minimal-loss betting strategies for cash washing is constrained by the physical and time-bound nature of on-course events, limiting the scale and sophistication of laundering schemes in this environment. Although it is common practice for on-course bookmakers to accept bets on other events besides the one they are physically attending.

[295] Horse Racing Ireland / Factbook Every Racing Moment 2024, Betting / Available from: https://www.hri.ie/HRI/media/HRI/Comms/Documents/HRI-Factbook-2024-FINAL-INTERACTIVE.pdf / p. 6
[296] Irish National Professional Bookmakers Association data
[297] Revenue data

Table 24: On-course Horse Racing Bookmakers (2020 – 2024)[298]

Year	Home	Away	SP Shop[299]	Total on-course Betting
2020	€6,835,393	€135,963	€1,333,881	€8,305,237
2021	€11,684,083	€538,719	€1,162,614	€13,385,416
2022	€56,734,605	€1,834,249	€8,906,545	€67,475,399
2023	€59,446,696	€2,373,656	€9,924,766	€71,745,118
2024	€63,136,557	€2,596,431	€9,632,830	€75,365,818

In 2024, there were 1,324 on-course greyhound racing meetings held across licensed stadia, attracting approximately 315,000 attendees. Greyhound Racing Ireland ("GRI") is responsible for issuing permits to on-course bookmakers, licensing tracks, and enforcing the rules of racing.

Vulnerabilities

The retail bookmaking sector vulnerabilities align with on-course bookmakers vulnerabilities above. These include a high prevalence of cash which makes it difficult to track aggregate spend for cash transactions to trigger CDD and may inhibit effective transaction monitoring. However, on-course bookmakers face significant challenges in monitoring activity in line with the CJA[300] due to the fragmented and fast-paced nature of the environment. Criminals can exploit this by placing multiple bets with different operators, within a short time frame. Unlike retail settings, on-course operators often lack the infrastructure to track cumulative spend across bookmakers, making it difficult to identify cash-washing activities. These operational limitations significantly increase the sector's vulnerability to ML.

Remote Betting Service Providers (Bookmakers, Exchanges and Intermediaries)

Risk Rating

Remote gambling service providers are assessed as posing a significant risk for ML, and low risk for TF and PF. The risk landscape across the remote channels is similar, as the deposit and withdrawals are primarily through digital payment platforms, for example Retail Banking products. This risk is significantly amplified when providers operate from outside Ireland or the EU without equivalent regulatory oversight, or through unlicensed platforms (black-

[298] Horse Racing Ireland / Factbook Every Racing Moment 2024, Betting / p.6
[299] The total turnover from bets placed in SP Shops (on-course betting outlets offering bets at Starting Price)
[300] Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 / Responsibilities of Designated Persons Section 33.

market platforms), facilitating opaque fund flows and increasing exposure to criminal activity beyond the reach of supervision.

Overview of Remote Bookmakers

In 2023, 79 licensed remote bookmakers were operating in Ireland (illustrated in figure 12), with the gross staking of remote bookmakers in Ireland estimated at €2.5 billion (illustrated in figure 13). For remote bookmakers and account-based customers,[301] identification and verification are typically conducted through digital platforms during account opening, and some firms use automated transaction monitoring systems. These systems are often also used to identify other concerns, such as problem gambling, match fixing, and advantage players.[302]

The larger retail bookmaking service providers in Ireland often integrate their retail operations with their remote bookmaking services. This integration allows online account holders to fund their accounts through retail bookmaker premises by depositing cash, over the counter, or transferring funds via self-service betting terminals available in the retail locations.

Vulnerability 1: White Labels

OCGs may seek to establish or acquire gambling operations as a front to launder money. One available mechanism to do so is using a 'white label', in which gambling services are provided under another company's brand, which can obscure the true operators and complicate regulatory oversight. White labels also make entry to the market more accessible for entrants, as they remove entry barriers such as technical knowledge, system requirements, and set-up costs.

Moreover, the high volume of transactions and the nature of gambling as a service with no physical product make it particularly attractive for ML. Accounts can be easily created and used to funnel illicit funds into the online bookmaker's business, often with limited scrutiny. This combination of anonymity due to insufficient CDD, accessibility, and transactional fluidity increases the risk of exploitation for ML purposes.

Vulnerability 2: Remote Nature of the Service Offering

Remote gambling involves customers who are not physically present and can be exploited by criminals who use counterfeit or stolen documents to bypass identity verification controls, allowing them to create accounts and conduct transactions under false identities. The ability

[301] Account-based customers are individuals who have registered for an account with a gambling provider either through their online services or retail premises.
[302] Advantage players, use legal methods to gain an edge in gambling, unlike cheating. They exploit inherent game characteristics to improve their chances of winning.

to create and manage multiple remote accounts can be exploited by criminals to spread and obscure their transactions, making it harder to detect patterns of ML.

Remote gambling firms are also exposed to ML methods commonly used against traditional financial institutions, such as money mules and structuring, as well as to specific gambling threats such as the use of third parties[303] and betting agents.[304] The use of these third parties can obscure the source or ownership of money gambled by customers and their identities which further complicates the detection and prevention of ML.

Where online gambling providers do not implement closed-loop payment systems,[305] accounts can be funded using multiple cards, while all funds (whether lodged or won) may be withdrawn by a single beneficiary.

Vulnerability 3: Means of Payment

Pre-paid cards offer users a convenient way to transfer funds to online gambling accounts, which can be exploited by criminals to move and launder money without detection. However, this risk is mitigated by the fact that there is a €150 limit on anonymous card purchases and such cards cannot be reloadable, therefore multiple cards would be required to launder any significant volumes, which should trigger an alert on the online gambling providers AML/CFT systems and controls.

Vulnerability 4: Inconsistent Regulatory Supervision Across Jurisdictions

Online gambling providers face elevated AML/CFT risks due to inconsistent regulatory standards across Europe. Operators licensed in less stringent jurisdictions can legally offer services in Ireland through the EU freedom of services rules, potentially circumventing Irish regulatory requirements. In addition, providers based entirely outside the EU may also target Irish customers without being subject to any EU-level supervision, creating further blind spots. These regulatory gaps can be exploited by criminal actors to facilitate ML and TF through cross-border gambling platforms, where financial transactions occur outside the scope of traditional regulatory oversight. While EU reforms aim to harmonise supervision,

[303] Third Parties: These can include intermediaries or agents who place bets on behalf of others. By using third parties, the actual source of the funds and the identity of the person placing the bet can be hidden. This makes it difficult for authorities to trace the origin of the money and identify the true owner.
[304] Betting Agents: These individuals or entities act as facilitators for placing bets. They can pool money from various customers and place bets in bulk. This aggregation of funds can further obscure the individual sources and owners of the money, complicating the detection of illicit activities.
[305] A closed-loop payment system is a payment arrangement where both the front-end (user interface) and back-end (processing infrastructure) are operated by the same entity, allowing transactions to occur exclusively within that system.

current inconsistencies continue to challenge effective risk management for Irish-licensed providers.

Private Members' Clubs

Risk Rating

PMCs are assessed as posing a significant risk for ML and a low risk for TF and PF. This elevated ML risk is driven by the cash-intensive nature of products and services offered, particularly poker and casino table games which create vulnerabilities. Additionally, there are lower levels of awareness and understanding of ML, TF, and PF obligations within this sub-sector, which further heightens the risk profile.

Overview of PMC

PMCs offer gambling services typically aligned with casinos (e.g. blackjack, roulette, and baccarat), poker games, and gaming machines (slot-style games). All PMCs offering live gaming are required to register with the AMLCU. As of June 2025, there were 12 registered PMCs in Ireland.[306] Irish PMCs are typically smaller operations compared to traditional casinos, with revenue not in excess of €5 million, and the majority reporting revenue below €1 million.[307]

Vulnerability 1: Cash-Intensive

PMCs are inherently cash-intensive operations. During a visit to a PMC, a customer may engage in multiple cash transactions at various stages, including the initial buy-in, during gameplay, or at the cash-out stage. Due to this operating environment, PMCs are inherently exposed to cash washing, as the high volume and fluidity of cash transactions makes it difficult to trace the origin and movement of funds.

This vulnerability is underscored by survey findings, which indicate that 87.5% of respondents accept cash payments. Over half of the respondents reported that cash transactions represent over 90% of their total transaction volume, and 50% reported having no cash deposit limits. Among the PMCs that reported not having established cash deposit limits, 50% stated that they do not verify the source of funds for any cash transactions, further highlighting the lack of due diligence performed on cash transactions.

[306] PMC Register 26-06-2026 / https://www.amlcompliance.ie/wp-content/uploads/2025/06/PMC-Register-26-06-2025.pdf
[307] Figures as per the survey responses

Vulnerability 2: Products and Services

The below products and services offered by PMCs presents specific vulnerabilities for ML:

- Poker, being cash-based and P2P, poses significant ML risks through collusion and manipulation.

- Casino table games, especially roulette and baccarat, enable structured or minimal loss betting strategies, which are attractive to criminals.

Vulnerability 3: PMCs' Ability to Implement Effective Controls

The small-scale operations of PMCs, coupled with a high level of cash transactions, pose significant challenges for effective AML/CFT compliance, via robust CDD procedures, hindering the detection of suspicious activities. Moreover, the effectiveness of AML/CFT controls can be compromised by insufficient staff competency and high turnover, which erodes institutional AML/CFT awareness and weakens compliance culture. As highlighted in recent AMLCU reports, persistently low compliance rates across the sector underscore the need for enhanced training, stronger governance, and sustained investment in AML/CFT capabilities.[308]

Vulnerability 4: PMCs Being Owned or Controlled by Criminals

PMCs may be acquired or influenced by criminals including OCGs as a means to launder the proceeds of crime. In some instances, employees may collude with criminal actors or be coerced through intimidation to facilitate ML. The club-like structure of PMCs, where staff often have personal familiarity with members, can create a reluctance to challenge or refuse service, even if there are suspicions regarding the source of funds. This dynamic increases the risk of illicit funds being accepted and processed without adequate scrutiny.

Compounding this risk is the high cash-intensive nature of PMCs and the way funds are exchanged through staking and payouts, rather than through the sale of a physical product. This transactional model can obscure the origin and flow of money, making it easier for illicit cash to be integrated into the legitimate financial system. These combined factors make PMCs particularly attractive for criminal exploitation and highlight the need for robust controls and oversight.

[308] AMLCU / 2024 – Annual Report on Anti Money Laundering Compliance Unit and 2023 – Annual Report on Anti Money Laundering Compliance Unit / Available from: https://www.amlcompliance.ie/annual-reports/

Lotteries and Bingo Operators

Risk Rating

The National Lottery and traditional in-person bingo operators are assessed as posing a low risk for ML, TF, and PF. These activities are generally unattractive for ML due to their reliance on chance, which limits the ability to manipulate outcomes.

National Context

The National Lottery is regulated by the Regulator of the National Lottery under the National Lottery Act 2013. Premier Lotteries Ireland, owned by La Française des Jeux, was licensed to operate the National Lottery from 30 November 2014 for 20 years. In 2023, the Irish National Lottery paid out €478.8 million which accounted for 54% of the revenue generated.[309] The Lottery offers a range of games, including scratch cards, raffles, bingo, digital games, and draw-based formats such as Lotto and EuroMillions. The National Lottery is assessed as posing a low risk for ML, TF, and PF.

Traditional in-person bingo is regulated under the Gaming and Lotteries Act 1956, where it is classified as a lottery. Operators must adhere to a weekly prize cap of €5,000 and a maximum ticket price of €10. However, this framework is set to evolve with the phased implementation of the Gambling Regulation Act 2024. Once in effect, traditional bingo operators will require a gambling licence from the GRAI, although exemptions may apply for charitable or low-stakes activities.[310] The traditional in-person bingo is assessed as posing a low risk for ML, TF, and PF.

Under the Gaming and Lotteries Act 1956, local lotteries in Ireland are generally prohibited unless conducted for charitable or philanthropic purposes. These may be authorised by An Garda Síochána or the District Court, though tracking registration numbers is difficult due to the absence of a centralised registry. Prize limits are capped at €5,000 per week for An Garda Síochána supervised lotteries and €30,000 for those licensed by the District Court.[311]

Small-scale charitable lotteries may operate without a licence if strict conditions are met, including limits on prize value (€2,000), ticket price (€5), and ticket volume (1,500), with no

[309] National Lottery / A Year in Review / Available at: https://cdn2.lottery.ie/uploads/NL_2023_Annual_Report_5b9d57dd50.pdf / p.21
[310] Department of Justice, Home Affairs and Migration / Gambling Regulation Act 2024 / Available from: https://www.gov.ie/en/department-of-justice-home-affairs-and-migration/publications/gambling-regulatory-authority-of-ireland/
[311] Gaming and Lotteries (Amendment) Act 2019, Section 11 & 12

personal profit and only one lottery allowed every three months. In contrast, online bingo operators must now obtain a gambling licence under the Gambling Regulation Act 2024.

Vulnerabilities

The Irish National Lottery exposure to ML is low, due to the low probability of winning major prizes (i.e.,1 in 10.7 million and 1 in 139.8 million for The National Lottery and Euro Millions respectively), and limited opportunities to manipulate the game, making large scale or coordinated ML economically unfeasible. This low risk is further mitigated as the National Lottery operates under specific regulations established by the National Lottery Act 2013, compliance with which is overseen by the Regulator of the National Lottery.

Local lotteries and bingo operators have limited capacity for ML and TF purposes, due to the reliance on chance and relatively small prizes. The main threat is of infiltration and control of local lotteries by bad actors.

Local lotteries in Ireland are permitted by a local Garda superintendent or licensed by a District Court, depending on the size of the prizes, and vetting is conducted on the fitness of the individuals involved in the lottery. Bingo operators are similarly required to be licensed, which creates a barrier to prevent criminal infiltration, however the absence of centralised records for licenses or permits complicates efforts to effectively monitor the scale of local lotteries and bingo activities.

The lack of opportunity and the presence of more feasible alternatives make ML/TF through the National Lottery and bingo operators unattractive, however local lotteries remain vulnerable to infiltration and control by bad actors.

The Tote

Risk Rating

The Tote is assessed as posing a low risk for ML, TF, and PF. Tote betting is generally unattractive for ML due to its pooled betting system and the absence of fixed odds, which limits manipulation. Additionally, the Tote service providers, HRI and GRI, are semi-State entities that have implemented significant AML/CFT measures, further reducing risk.

National Context

The Tote in Ireland is operated by two semi-State bodies, the GRI and HRI, under the Totalisator Act 1929.[312] Tote betting requires all wagers to be pooled, with winners sharing the pool after the operator deducts a commission. The payout is determined by the total amount wagered in the pool and the number of punters who bet on each horse, with fewer winning bets resulting in higher payouts for each winning punter. Tote Ireland, owned by HRI, manages on-course and pool betting, generating an annual pool handle[313] of €71 million, including €10 million from on-course betting.[314]

Vulnerabilities

The risk of ML on the Tote stems from its cash-intensive nature, the potential for launderers to purchase winning tickets, and the risk of criminal infiltration. However, as the Tote betting providers do not offer fixed odds, there is limited opportunity for criminals to employ betting strategies for guaranteed returns. The average wager for Tote providers in Ireland remains low (estimated at €6.50),[315] with large-scale wagers likely attracting attention due to limits per teller and the irregularity of high value bets. The HRI and GRI operate under semi-State ownership and have risk-based AML and CFT oversight mechanisms in place, reducing the risk of criminal infiltration.[316]

Case Study: A case of gambling-driven embezzlement

In 2025, a financial administrator at a private secondary school in Dublin was prosecuted for embezzling approximately €500,000 from the school's accounts between 2012 and 2017, to fund gambling activities. The individual exploited their position by manipulating accounting records, falsifying lodgement entries, and diverting funds intended for school operations into personal accounts. As the designated signatory on bank accounts and the person responsible for maintaining financial records, the administrator had both the access and opportunity to carry out the fraud over an extended period. In this case, the stolen funds were not laundered through gambling platforms, but rather used directly to support the individual's gambling habits. This highlights the role of gambling providers in detecting and responding to potentially harmful or criminal behaviour, reinforcing the need for strong due diligence, transaction monitoring, and responsible gambling practices.

[312] Totalisator Act 1929 - https://www.irishstatutebook.ie/eli/1929/act/22/enacted/en/html
[313] A pool handle refers to the total amount of money wagered in a betting pool. This includes all bets placed on a particular event or series of events, and the pool handle is used to determine the payouts for winning bets.
[314] Horse Racing Ireland / Factbook Every Racing Moment 2024, Betting / p.7
[315] As per engagement with HRI
[316] As per submissions and engagement with HRI and GRI

Consequence

The gambling sector in Ireland supports employment and contributes to the wider economy, although its societal impacts include both economic benefits and recognised challenges. While a substantial ML, TF or PF incident in the sector could raise reputational concerns and affect market integrity due to its visibility and societal reach, the overall impact on financial systems, national interests and society would likely be limited. As such, consequence has been rated as moderate.

EU Supranational Risk Assessment

The EU Supranational Risk Assessment breaks down the gambling industry into six categories and assessed them in the most recent (2022) risk assessment as per the below:

Sub-Sector	TF Risk	ML Risk
Betting (offline)	Not Relevant	Significant
Bingo (offline)	Not Relevant	Lowly Significant
Casino (offline)	Not Relevant	Moderate
Lotteries	Not Relevant	Moderate
Poker	Not Relevant	Significant
Online Gambling	Very Significant	Very Significant

The risk factors identified within this sectoral risk assessment are aligned with those set out in the EU Supranational Risk Assessment, with the exception of online gambling.

Horizon Scanning

The 6th AML Directive allows EU Member States to adopt national rules in areas not fully harmonised at the EU level, such as online gambling, provided these rules serve a public interest, are non-discriminatory, and proportionate. However, AMLD6 has not yet been transposed into national legislation, with a deadline set for 10 July 2027.

The adoption of cryptocurrencies and assets as a source of funds or a payment option by gambling providers presents significant risks due to their high degree of anonymity and the ability to rapidly transfer large sums of money. As the use of virtual assets as a whole and within the gambling industry grows, it is crucial for gambling operators and regulators to ensure appropriate measures are taken to mitigate these risks effectively. Some gambling service providers in the UK currently accept cryptocurrencies; if their move towards cryptocurrencies proves successful, other market players (including in Ireland) may seek to follow suit and offer similar services.

The prevalence of unlicensed (black market) gambling operators remains a persistent issue in Ireland[317] and is well documented across the EU.[318] Black-market gambling providers do not operate under the required regulatory and legal obligations, presenting risk in relation to ML, criminal activities and tax evasion.

Through discussions with industry stakeholders, it was noted that small-scale gambling providers had been unable to access banking services, likely as a result of some banks' limited risk appetite for onboarding gambling providers. This trend may push gambling service providers towards alternative solutions, which can increase the risk of ML, TF, and PF due to less robust controls adopted in these firms, making it easier for illicit activities to go undetected.

[317] As per engagement with the wider industry
[318] Betting and Gaming Council / Available from: https://bettingandgamingcouncil.com/news/new-research-reveals

High Value Goods Dealers

Executive Summary

	2019 Risk Ratings	2026 Risk Ratings
ML	Medium-High	Significant
TF	Medium-High	Significant
PF	Not Assessed	Low

Key Insights

Due to the nature of high-value goods, this sector is inherently attractive to ML and TF activities. The combination of high-value items, ease of transfer, and the potential for anonymity in transactions makes these goods particularly vulnerable to misuse. HVGs can be exploited by criminal means to store or transfer illicit value, serve as a symbol of status or lifestyle, and represent a final objective of criminal activity, particularly for items such as luxury watches and high-end vehicles.

The key vulnerabilities within the sector are as follows:

- **Challenges in tracking linked transactions:** Manual tracking and sporadic customer interactions make it difficult to detect linked transactions over €10,000, increasing the risk of illicit actors structuring transactions to avoid detection.

- **Store of value and ease of transfer:** HVGs can often be easily transported (including across borders) and often retain or increase in value.

- **Gaps in understanding of AML/CFT obligations:** Results of inspections carried out on HVGDs by the AMLCU between 2023 and January 2025 suggest firms lack awareness of their AML/CFT obligations.

- **Ownership and use of HVGDs by criminals:** As well as the HVGs being used to store and transfer value, HVGDs themselves can be used as fronts for OCGs.

Legislative and Regulatory Framework for the HVGs sector

HVGDs are “designated persons” under the CJA and are defined as “any person trading in goods, but only in respect of transactions involving payments, to the person in cash, of a total of at least €10,000 (whether in one transaction or in a series of transactions that are or appear to be linked to each other)”.

AMLD6 will introduce substantive changes in the scope of designated persons in the HVGD sector as outlined in the horizon scanning section below.

Scale and Structure of the HVGs Sector in Ireland

There is currently no definition of HVGD in the CJA which confirms in-scope sectors or products; however, for the purposes of this assessment, jewellers, bullion dealers, antique dealers, motor and heavy machinery dealers, art dealers, and luxury goods dealers[319] have been assessed. HVGDs are not obliged to register with the AMLCU. However, as of February 2025, the AMLCU has a record of 2,975 HVGDs operating in Ireland.

The table below illustrates the numbers extracted from the AMLCU's database as of February 2025. The exact percentage of firms in each sub-sector from the database, relative to the total population of firms, is not currently available. However, this will be addressed when AMLD6 is transposed into Irish law through amendments to the CJA as it will introduce a requirement for all obliged entities, as defined under the package, to register.

Table 25: Breakdown of HVGDs as per the AMLCU database[320]

HVDG Breakdown	
Art Intermediary	4
Horse Transportation	6
HVGD Manufacturing Building	7
Motorbikes	16
Gold Bullion Dealer	24
HVGD Kitchens	24
HVGD Luxury Retail	28
Plant Hire and Sales	54
HVGD Monuments	66
HVGD Uncategorised	127
Marine Dealers	111
Antique Dealer	115
Art Traders	179
Art Dealers	195
Jewellers	369
Car Dealer	1650

[319] Referred to as designer goods by Law enforcement and luxury good dealers by the AMLCU
[320] Data as at February 2025

Jewellers

The jewellery sector in Ireland consists of both independent jewellers and larger retail chains. Jewellery is attractive for illicit finance as items are small, capable of being concealed and transferred across borders, and for certain items are a good store of value.

Bullion Dealers

Bullion dealers trade in high-value precious metals, such as gold and silver. These assets are highly liquid, easily transported and retain significant intrinsic value, which makes them inherently vulnerable to misuse.

In 2023, law enforcement held the first publicly advertised online auction of confiscated high value luxury goods, including watches, jewellery, gold bars and designer goods and generated a total of €446k.[321]

Antique Dealers

Antique dealers trade in a wide variety of items, including furniture, coins, jewellery, fine art, etc. The trade in antiques presents risks as these goods are portable and objective valuation is difficult to establish, which can assist in the transfer of illicit funds (e.g. by over/under invoicing to transfer funds). According to the Irish Antique Dealers Association (which represents 90% of antique dealers in Ireland),[322] it is estimated that half of its members handle goods with a sale value exceeding €10,000; however, cash transactions are rare.

Car and Heavy Machinery Dealers

This sub-sector includes businesses involved in the sale of new and used cars, as well as agricultural and farm machinery equipment. These items often hold significant resale value, and may be traded internationally, making them potentially attractive for ML, TF, and PF. Law enforcement data (Table 26) shows a decline in the total value of vehicles frozen from 2022 to 2023; however, this increased again in 2024. Law enforcement still view high end cars as a common ML mechanism, as well as being a lifestyle choice for criminals.

[321] Criminal Assets Bureau / Annual Report 2023 / Available from: https://www.cab.ie/wp-content/uploads/2024/10/CAB-Annual-Report-2023-Final.pdf / p.23

[322] Statement made during an interview with the Irish Antique Dealers Association / 25 February 2025.

Art Dealers

Although the global art market is significant, estimated at $65 billion[323] in 2024, the commercial art market in Ireland is relatively small, with only a small number of galleries and auction houses operating nationwide, and not all of these will conduct high value transactions. As highlighted by the FATF, "*there is a culture of privacy and discretion regarding the identify of buyers and sellers*"[324] which can inhibit the traceability of transactions in this market. Therefore, while the scale of the market in Ireland is modest, it remains susceptible to misuse.

Luxury Good Dealers

The mobility, anonymity, and resale potential of luxury fashion items increases their attractiveness for ML and TF purposes. While most designer goods transactions occur via established retail channels, there is also a portion of the resale market that operates through less regulated or informal platforms (for example though social media platforms), which limits the traceability of transactional activity. As noted in Table 26, there has been a significant amount in terms of numbers and values of CAB seizures involving designer goods in recent years.

Threats and Vulnerabilities

Threats

The ML, TF, and PF threats to which Ireland is exposed are assessed above. The HVG sector is exposed to a range of criminal threats, particularly fraud and extortion, bribery and corruption and illicit trade and smuggling. These sub-sectors facilitate the storage and transfer of value through high-priced goods, making them attractive vehicles for laundering proceeds of crime. Criminal networks exploit the sector's ability to move significant value discretely and cross-border, often using fraud and extortion schemes to acquire goods or manipulate transactions. Parts of the HVGs sector, such as antique dealers and art dealers may be exposed to underlying threats related to illicit trafficking and cultural goods, although current evidence suggests this is not a significant threat in Ireland. The FATF has also highlighted that dealers in precious metals and stones are among the sectors with higher

[323] Art Basel / The Art Basel and UBS Global Art Market Report 2024 / Available from: https://www.ubs.com/global/en/our-firm/art/art-market-insights/download-survey-report-2024.html
[324] FATF / Money Laundering and Terrorist Financing in the Art and Antiquities Market / p.3

exposure to potential breach, non-implementation or evasion of TFS related to PF,[325] which can be facilitated through the ease of transfer of such goods.

A total of 101 STRs were submitted by firms in this sector in 2024, Of those which have been fully analysed, ≈7% were disseminated to law enforcement for further investigation. Of the 101 STRs submitted in 2024 approximately 80% selected 'ML' as the reason for submission.

HVGs are used both as tools for ML and as end goals of criminal activity, in particular high-end vehicles, luxury watches and designer goods. These goods have been seized as part of policing operations, with a notable trend toward the seizure of designer goods from 2022 to 2023, as shown in Table 26 below.[326]

Table 26: Assets over which orders were made[327] and value of assets frozen (2020 – 2024)[328]

Category of Assets	2020	2021	2022	2023	2024
Jewellery Orders	19	16	22	16	1
Jewellery Value Frozen	€226,520	€107,231	€222,350	€171,645	€9,000
Vehicles Orders	14	96	18	15	19
Vehicles Value Frozen	€254,687	€1,078,760	€412,589	€378,708	€276,502
Designer Goods Orders	28	5	37	128	2
Designer Goods Value Frozen	€49,344	€13,700	€31,495	€144,796	€3,000

[325] FATF / Complex PF Sanctions Evasions Schemes / p.20
[326] Figures from CAB annual reports and reflect seizures under CAB's non-conviction based asset forfeiture model. These figures do not include high-value goods seized through post-conviction criminal investigations, and therefore may not represent the full extent of asset seizures.
[327] Assets over which section 2(1) orders were made under the Proceeds of Crime Act 1996 to 2016
[328] Assets frozen under section 2 of the Proceeds of crime act 1996 to 2016

Vulnerabilities

In assessing the vulnerabilities of the HVGDs sector the assessment considered FATF guidance and the results of the EU Supranational Risk Assessment, as well as information obtained from regulators, law enforcement and participants within the sector.

Vulnerability 1: Challenges in Tracking Linked Transactions

Transactional activity in the HVGD sector can be largely one-off purchases, with sporadic customer interactions. This makes it difficult to establish patterns of behaviour, and to detect linked transactions that exceed €10,000. Where cash is used, there is further difficulty in the tracking and tracing of transactional activity.

Some more mature firms in the sector use sales and customer management systems to do so, while others rely on manual processes. Results from the motor industry survey showed that ≈40% relied solely on manual tracking, ≈3% did not track at all, and the rest had some form of automated tracking systems. The absence of an automated tracking system makes it more difficult to spot patterns, such as structuring of transactional activity, or the use of intermediaries. Without robust tracking, illicit actors may exploit this by making multiple transactions below the €10,000 threshold to avoid detection. In addition, the use of intermediaries and/or complex ownership structures in purchases of HVGs can inhibit the ability of HVGDs to identify linked transactions. This risk is somewhat mitigated as HVGDs may need to utilise other regulated firms (such as credit institutions) for services such as deposits and movements of funds. These firms will conduct due diligence and investigations where indicators of ML and TF exist – for example significant cash deposits, and will report suspicions to FIU Ireland.

Vulnerability 2: Store of Value and Ease of Transfer

HVGs can often be easily transported and generally maintain or in some instances appreciate in value, which increases the risk of their use in illicit finance. In discussions with law enforcement, it was noted that high value jewellery – in particular luxury watches – is a common store of value and lifestyle choice for criminals. These items are often bought or traded on social media, thereby avoiding the regulated HVGDs environment. Law enforcement also reported that private safety deposit boxes have been regularly identified during criminal and proceeds of crime investigations as being used by OCGs to store HVGs. Additionally, law enforcement has noted cases in which these items were being exported as a mechanism of moving assets internationally for OCGs. As well as being useful as a store of value, the difficultly in accurately pricing some HVGs can also be attractive for use in illicit

finance schemes, as criminals can overvalue or otherwise manipulate the price of goods to obscure the true value and enable the laundering of funds.

The formal Irish HVGD market is, however, primarily a domestic one. According to responses to the motor industry survey, only ≈4% of respondents operate internationally, while ≈2% engage in both international and domestic trade. In relation to other sub-sectors, industry associations for antiques dealers noted international trade is limited, primarily due to shipping difficulties and custom delays. However, importation and distribution of agricultural machinery is more common.

Vulnerability 3: Gaps in Understanding of AML/CFT Obligations

Understanding of, and frameworks to prevent ML, TF, and PF in the HVGD markets are not well embedded across the industry. Of the 358 inspections by the AMLCU in 2023 of HVGDs, 25% resulted in compliance rates of either 'partially compliant' or 'non-compliant'. In respect of the AMLCU reviews carried out between 2023 and 2025, enforcement actions issued suggest firms lack awareness of their AML/CFT obligations. Approximately 32% of actions issued identified training as a deficiency, while 45% flagged weakness in CDD. This is further supported by the findings of the motor industry survey, with 28 of the 82 respondents stating that their staff do not receive training on financial crime risks and legislation in Ireland. This challenge is not unique to Ireland and was referenced in the rationale for making updates in the 6th AML package.[329] Law enforcement intelligence indicates that high street purchases of high-value goods, both new luxury items and second-hand "grey market" products like vehicles and watches, are a significant method for laundering criminal proceeds. Daigou-linked[330] purchases by facilitators exiting the country are of particular concern, which could be partially addressed through stronger compliance measures among retailers.

[329] (Regulation; 18) "Directive (EU) 2015/849 set out to mitigate the ML and TF risks posed by large cash payments by including persons trading in goods among obliged entities where they make or receive payments in cash above €10 000, whilst allowing Member States to introduce stricter measures. Such an approach has shown to be ineffective in light of the poor understanding and application of AML/CFT requirements, lack of supervision and limited number of suspicious transactions reported to the (FIU). In order to adequately mitigate risks deriving from the misuse of large cash sums, a Union-wide limit to large cash payments above €10 000 should be laid down. As a consequence, persons trading in goods no longer need to be subject to AML/CFT obligations, with the exception of persons trading in precious metals, precious stones, other high value goods and cultural goods".

[330] Individuals who purchase goods, often luxury items, overseas and resell them in China, typically at a profit

Vulnerability 4: Ownership and Use of HVGDs by Criminals

More sophisticated criminals – including OCGs – may directly own or control HVGD businesses. Their cash-intensive nature, the high value of the underlying goods being traded, and less regulatory oversight make them attractive fronts for illegal activity. Recent law enforcement activity shows that OCGs are using HVGDs in this way, both within Ireland and internationally.

Case Study

Gardaí investigating an OCG in south Dublin seized 29 cars from a car sales business suspected of laundering money for the criminal group in March 2025.

The cars, valued at up to €600,000, were part of a broader investigation into drugs-related ML and fraud offences. Additionally, €200,000 in cash was frozen in company accounts, believed to be proceeds of crime.

Consequence

The HVGD sector encompasses a wide range and significant number of businesses. Although a significant ML, TF, or PF incident within the sector could undermine the integrity of the market and damage Ireland's reputation internationally, this would likely be limited. As such, the consequence has been rated as low.

EU Supranational Risk Assessment

The EU Supranational Risk Assessment breaks down the HVG sector into three categories and assessed them in the most recent (2022) risk assessment as per the below:

Sub-Sector	TF Risk	ML Risk
HVGs – artefacts and antiquities	Significant	Significant
High value assets – Precious metals and precious stones	Significant	Significant
High value assets – other than precious metals and stones	Not Relevant	Significant

The risk factors identified within this sectoral risk assessment are aligned with those set out in the EU Supranational Risk Assessment.

Horizon Scanning

AMLD6, published in 2024, introduces changes to the scope of the regulated HVGDs sector. AMLD6 sets specific thresholds for persons trading in precious metals, precious stones, other HVGs and cultural goods. These categories are defined as follows:

- **HVGs:** means jewellery, gold or silversmith articles, clocks and watches exceeding €10,000; motor vehicles exceeding €250,000; aircraft and watercraft exceeding €7,500,000.

- **Precious metals:** Gold, Silver, Platinum, Iridium, Osmium, Palladium, Rhodium and Ruthenium.

- **Precious stones:** Diamond, Ruby, Sapphire and Emerald.

- **Cultural goods:** Goods listed in Annex I to the Council Regulation (EC) No 116/2009.[331]

HVGDs outside of these categories may no longer be subject to AML/CFT obligations. However, Article 3 of the Directive sets out a formal process for adding additional cohorts to the list of obliged entities where Member States identify entities in other sectors which are exposed to ML/TF risks. Furthermore, entities captured by the legislation will be obliged to comply with the requirements of the regulation regardless of the form of payment. To ensure that the measures remain proportionate to the risks posed by transactions below €10,000, obliged entities will be required to complete due diligence limited to the identification and verification of the customer and the beneficial owner when carrying out occasional cash transactions of at least €3,000. Furthermore, to mitigate the risks posed by large cash payments, an EU-wide limit will be introduced, effectively prohibiting cash payments exceeding €10,000.

Once transposed into Irish law through amendments to the CJA, these changes will alter the boundary of designated persons constituting HVGDs. As a result, new firms brought into scope will need to implement appropriate compliance frameworks to comply with the requirements.

[331] European Union / Official Journal of the European Union / Available from: https://eur-lex.europa.eu/eli/reg/2009/116/oj/eng

The increasing use of online marketplaces and social media for the sale of high-value items like jewellery, watches, and luxury fashion introduces new AML/CFT challenges. For instance, platforms like Instagram and TikTok have become key channels for showcasing luxury goods, with features such as live shopping and influencer partnerships driving consumer interest. These platforms frequently lack controls or traceability of transactions, facilitating the transfer of value or concealment of fund origins through anonymous or pseudonymous transactions by illicit actors. HVG sales through social media are not subject to any regulatory oversight, and accounts selling goods are often transient in nature, with some existing for only a short period, before disappearing. This lack of stability and formal accountability further exacerbates the challenges of identifying and addressing financial crime facilitated through social media.

Legal Persons and Arrangements

Executive Summary

	2019 Risk Ratings	2026 Risk Ratings
Companies		
ML	Medium-High	Significant
TF	Medium-High	Moderate
PF	Not Assessed	Low
Special Purpose Entities (SPEs) – SPE Securitisation		
ML	Medium-High	Significant
TF	Medium-Low	Moderate
PF	Not Assessed	Low
Special Purpose Entities (SPEs) – SPE Non-Securitisation		
ML	High	Very Significant
TF	Medium-Low	Moderate
PF	Not Assessed	Low
Express Trusts - Welfare and Community Trusts		
ML	Low	Low
TF	Low	Low
PF	Not Assessed	Low
Express Trusts - Pension Purpose Trusts		
ML	Low	Low
TF	Low	Low
PF	Not Assessed	Low
Express Trusts - Employee Share Schemes		
ML	Low	Low
TF	Low	Low
PF	Not Assessed	Low
Express Trusts - Charitable Trusts[332]		
ML	Medium-Low	Low
TF	Medium-Low	Moderate
PF	Not Assessed	Low
Express Trusts - Express Trusts (Other)		
ML	Medium-Low	Moderate
TF	Medium-Low	Moderate
PF	Not Assessed	Low
Partnerships		
ML	Medium-Low	Moderate

[332] As defined in Section 2 of the Charities Act 2009

	2019 Risk Ratings	2026 Risk Ratings
TF	Low	Low
PF	Not Assessed	Low

A comprehensive risk assessment of legal persons was conducted as part of the 2026 NRA process, the results of which reaffirmed the key findings of a previously conducted standalone legal persons and arrangements risk assessment.[333] The information contained in this chapter is focused on providing updates to the more substantive information relating to the nature of the legal persons, and the associated ML, TF, and PF vulnerabilities of these entity types which is contained in the 2020 document, as well as the information contained in Appendix 2. This chapter should also be read in conjunction with the funds sectoral risk assessment as taken together they provide an assessment of the risks to Ireland from, inter alia, foreign legal vehicles with a sufficient nexus to Ireland.

Key Insights

The vulnerabilities of legal persons and arrangements, both those formed in Ireland and those originating elsewhere but with operations in Ireland, remain consistent with those identified in the previous risk assessment:

- **Opaque and Complex Ownership Structures:** This can include establishing ownership across multiple jurisdictions, using intermediaries or nominees to obscure ownership, and the use of offshore companies in countries with less rigorous transparency requirements.

- **Misuse of Legal Person structures to operate illicit businesses:** Using legal persons as front companies, including using entities where oversight requirements are less stringent, and in sectors that are cash-intensive or inherently international.

- **Exposure to High-Risk Jurisdictions:** Legal persons enable the creation of links with overseas jurisdictions, including with high-risk jurisdictions, and those with sanctions regimes applied against them.

- **Verification of information submitted to beneficial ownership registers:** There is limited ability for those administering beneficial ownership registers in Ireland to verify information provided to them, which weakens the effectiveness of these registers.

[333] Department of Finance / Legal Persons and Legal Arrangements Risk Assessment / Available from: https://assets.gov.ie/static/documents/legal-persons-and-legal-arrangements-risk-assessment.pdf

- **Shell Companies:** Shell companies in complex corporate structures have been consistently used by criminal groups.

Changes have been made to the legislative framework for legal persons and arrangements since the previous legal persons assessment in 2020, including the creation of the Central Register of Beneficial Ownership of Trusts ("CRBOT"), a beneficial ownership registry for both Irish trusts and foreign trusts with a sufficient Irish nexus,[334] and the Beneficial Ownership Register of Certain Financial Vehicles ("BORCFV"), a beneficial ownership registry for certain types of fund sector legal structures in Ireland. In addition, the Corporate Enforcement Authority ("CEA") was established in 2022. For more information on CEA please see information contained in Table 9 of this document.

Beneficial Ownership Registers

In Ireland, there are three beneficial ownership registers, which have been established in alignment with the EU AML requirements.

- **Central Register of Beneficial Ownership Companies and Industrial & Provident Societies ("RBO"):** Established under S.I. No. 110/2019, the RBO requires entities to submit beneficial ownership details upon incorporation. The RBO is administered by the Companies Registration Office.

- **Central Register of Beneficial Ownership of Trusts:** Established under S.I. No. 194/2021, CRBOT requires trusts to report details on trustees, settlors, beneficiaries, and other relevant parties. The CRBOT is administered by Revenue.

- **Beneficial Ownership Register of Certain Financial Vehicles :** Established under S.I. No. 233/2020 (as amending the 2019 Regulations), and the Investment Limited Partnerships (Amendment) Act 2020, the BORCFV register covers, Irish Collective Asset-Management Vehicles, Unit Trusts, Credit Unions, Investment Limited Partnerships, and Common Contractual Funds. The BORCFV register is administered by the Central Bank.

[334] Not all foreign trusts are covered — only those with a relevant Irish nexus, meaning those from outside the EU, which are therefore not already subject to equivalent obligations in other EU Member States, but which enter into a business relationship or acquire land in Ireland.

Interconnection of Registers

While significant progress has been made nationally toward enabling interconnection via the Beneficial Ownership Registers Interconnection System ("BORIS"), Ireland's registers are not yet fully connected to this central platform. Each register is managed by a separate authority and operates on distinct IT systems, data formats, and access protocols. When all EU member state BO registers are fully connected to BORIS, competent authorities and designated bodies across the EU will have access (unrestricted and restricted as applicable) to pan-European BO information. Engagement with the European Commission is ongoing through the Department of Finance, with the aim of establishing interconnection at the earliest opportunity. However, key data protection issues remain unresolved and must be addressed before integration can proceed. In addition, access to the three registers is restricted to:

- Competent authorities (e.g. An Garda Síochána, FIU Ireland, Revenue, CAB) have unrestricted access to all registers.
- Designated persons under AML legislation may access data for due diligence purposes.
- Public access is restricted across all registers following a 2022 ECJ ruling, and access is only granted on a case-by-case basis where a legitimate interest can be demonstrated.

Companies

Risk Rating

Companies are assessed as posing a significant risk for ML and TF, and a low risk for PF.

Ireland recognises several company types under the Companies Act 2014, including:

- **Private Company Limited by Shares ("LTD"):** LTDs are the most common company type in Ireland (89% of all registered companies), offering limited liability and flexible governance. They pose the most significant ML and TF risk both domestically and internationally due to their ease of incorporation and widespread use in cash-intensive sectors.
- **Company Limited by Guarantee ("CLG"):** CLGs are typically used by not-for-profits and charities and do not have share capital.

- **Unlimited Company:** Unlimited companies may be exempt from filing financial statements unless all members are limited.[335]

- **Designated Activity Company ("DAC"):** DACs have defined objects in their constitution and exist in share or guarantee-limited forms. They pose both a domestic and international ML risk, particularly where used in financial or holding structures.

- **Public Limited Company ("PLC"):** PLCs sell shares to the public and are typically listed on a stock exchange. A PLC is commonly used for larger businesses, including investment firms and multinational corporations. PLCs are subject to strict regulatory requirements, including public disclosure of financial information and governance structures, which help mitigate ML and TF risks.

- **European Economic Interest Grouping ("EEIG"):** EEIGs are cross-border entities governed by EU regulations and are exempt from filing financial statements. They present a ML risk internationally due to their structural opacity and cross-border nature.

Scale of Company Structures in Ireland

Table 27: Comparison of Company Incorporations in Ireland (2019 vs 2023)[336]

Company Type	Total Incorporations as of 2019	Total Incorporations as of 2023	Percentage Change (+/-)
Private Company Limited by Shares	205,494	263,989	+28%
Companies Limited by CLG	16,535	18,623	+13%
Unlimited Companies (Private & Public)	4,644	5,203	+12%
DAC (Limited by Shares)	5,069	6,771	+34%
DAC Designated Activity Company (Limited by Guarantee)	100	91	-9%
PLC	454	490	8%
EEIG	24	26	8%

[335] If any member is a limited liability entity (e.g., a limited company), the unlimited company must file financial statements. This prevents using an unlimited company structure to hide financial information while shielding members from liability.
[336] Companies Registration Office data

Special Purpose Entities ("SPEs")

Risk Rating

Securitisation SPEs are assessed as posing a significant ML risk, while non-securitisation SPEs pose a very significant ML risk due to their broader business models (for example raising of debt, provision of loans or acting as part of a wider credit intermediation chain). Both types are assessed as posing a moderate TF risk and low PF risk.

Nature of SPEs

Irish SPEs are broadly categorised into two types: securitisation SPEs, also known as Financial Vehicle Corporations ("FVCs"), and non-securitisation SPEs, commonly referred to as "other SPEs". Section 110 SPEs have reporting obligations to the Central Bank (though not all SPEs are section 110 entities).

SPEs are a key part of Ireland's financial sector and play an important role in dispersing risk across the global financial system.[337] These legally distinct entities are typically established for narrow, specific, or temporary objectives and often operate as subsidiaries within broader international corporate structures and may have no physical presence or employees in Ireland. Close to 10% of Ireland's external assets are accounted for by SPEs,[338] with only Malta, Cyprus, Luxembourg, and the Netherlands having a larger percentage within the euro area. SPEs are typically established by the originator, sponsor or another related party to the transaction, who is considered legally separate from the SPE. One of the related entities will be designated the responsible party for accounting, legal or regulatory purposes While SPEs use orphan structures, the contract for the establishment and function of the SPE is drawn up by the aforementioned connected entity, and the directors of the SPE operate in accordance with that contract.

Ireland's section 110 taxation regime was designed to offer a tax neutral regime for certain securitisation. Due to an awareness of the risk that this regime could be used for other activities, a broad review of the section 110 regime is being carried out by the Irish government. This is to identify enhancements to the section 110 regime to ensure that the tax regime supports beneficial activities and cannot be abused for other purposes. This review is being undertaken alongside a major domestic project to reform Ireland's business

[337] Central Bank of Ireland / Economic Letter / Available from: https://www.centralbank.ie/docs/default-source/publications/economic-letters/vol-2018-no-11-shining-a-light-on-special-purpose-entities-in-ireland-(golden-and-hughes).pdf / p.3
[338] European Central Bank Eurosystem / ECB Data Portal / Available from: https://data.ecb.europa.eu/blog/blog-posts/understanding-relevance-special-purpose-entities-across-euro-area

interest taxation regime. These reforms are expected to reduce the use of section 110 vehicles for non-securitisation purposes.

The Funds Review report published the Minister for Finance in October 2024 included an examination of the use and scope of the section 110 regime and suggested recommendations to enhance the transparency of the section 110 regime.[339] These recommendations are being progressed as part of this broader review of the section 110 regime.

Scale of SPEs in Ireland

Irish-tax resident SPEs have experienced sustained growth over recent years, both in terms of the number of entities and the value of assets held. As of 2024, the total assets under management reached €1,147 billion, up from €893 billion in 2019, an increase of 32%. Over the same period, the number of SPEs rose from 2,603 to 3,608, representing a 39% growth in five years.[340]

In the securitisation sector, SPEs' total assets grew from €479 billion in 2019 to €666 billion in 2024, an increase of 39%. Non-securitisation SPEs also saw a rise in assets, from €393 billion in 2019 to €482 billion in 2024, reflecting a 23% growth over the same period.

Express Trusts

Irish law does not recognise or govern legal arrangements other than express trusts, whose trustees are resident in Ireland, or which are otherwise administered in Ireland, although Irish courts will recognise foreign registered and properly established legal arrangements. There are also no particular features of express trusts governed under Irish law which make them more vulnerable to misuse than trusts governed under other countries' laws, such as specific secrecy or asset flight features.

Risk Rating

This assessment examines risks in relation to Express Trusts established for specific purposes, including: (1) Welfare and Community purposes, (2) Pension purposes, (3)

[339] Department of Finance / Funds Sector 2030 / funds-sector-2030-a-framework-for-open-resilient-and-developing-markets.pdf
[340] Central Bank of Ireland, Special Purpose Entities Statistics, Q4 2019 and Q4 2024 / Available from: https://www.centralbank.ie/docs/default-source/statistics/data-and-analysis/other-financial-sector-statistics/financial-vehicle-corporations/2025q1-irish-special-purpose-entities.pdf?sfvrsn=b82d681a_4
Central Bank of Ireland, Special Purpose Entities Statistics, Q4 2019 / Available from: https://www.centralbank.ie/docs/default-source/statistics/data-and-analysis/other-financial-sector-statistics/financial-vehicle-corporations/spe-statistical-release-q4-2019.pdf?sfvrsn=6

Employee share schemes, (4) Charitable activities (5) Express Trusts (Other) - all express trusts other than those listed above. As noted in the 2020 assessment, resulting trusts, and constructive trusts pose a very limited risk of misuse for ML or TF, statutory trusts such as those established under the Succession Act 1965 are not considered to be trusts which can pose an ML or TF risk.

Welfare and Community Trusts,[341] Pension Purpose Trusts, and Employee Share Schemes are assessed as posing a low risk for ML, TF, and PF. These trusts are purpose-driven, with clearly defined objectives and limited financial complexity. They typically operate under strong governance frameworks, with transparent funding and low exposure to high-risk transactions.

Express Trusts (Other) are assessed as posing a moderate risk for ML and TF, while posing a low risk for PF. These trusts serve broader or more flexible purposes and may involve more complex financial flows or less standardised oversight. Charitable Trusts are covered within the NPO chapter as a subset of the NPO sector, they are rated as having low ML and PF risk and as posing moderate risk for TF.

Nature of Express Trusts

Express trusts in Ireland are typically established through the services of professional trustees, such as solicitors, accountants, or TCSPs, all of whom are designated persons under the CJA, and subject to AML/CFT obligations. They are also required to be registered with CRBOT. Express trusts may, however, also be created and administered by non-professionals.

Scale of Trusts in Ireland

- Express Trusts: Commonly established by professional trustees (e.g. lawyers, accountants, TCSPs) subject to AML/CFT obligations. As of September 2025, 19,431 trusts were registered with the CRBOT, a 129% increase from 2022.

- Pension Trusts: Widely used for occupational and personal pensions. In 2022, there were 85,228 active defined contribution schemes with 425,163 members, and 636 defined benefit schemes serving 549,858 members.

[341] Welfare and Community Trusts are charitable trusts established to support social welfare, community development, and related public benefit activities. They are typically made up of trustees, trust property/funds, and a legally binding charitable purpose such as poverty relief, education, health, housing, or community services.

- Welfare & Community Trusts: This is a large category which encompasses charities, sports bodies, trusts for voluntary and community purposes including student unions and trade unions.

- Employee Share Schemes: In 2022, APSSs[342] supported around 49,200 employees with an annual fiscal cost of €80 million. ESOTs[343] supported 7,000 employees, down from 11,900 in 2018, with an annual cost of €0.1 million.

- Charitable Trusts: Supervised by the Charities Regulator. As of 2024[344], 571 charitable trusts were registered, an 8% decrease from 2020.[345]

Partnerships

Risk Rating

Partnerships are assessed as posing a moderate risk for ML and a low risk for TF and PF.

Nature of Partnerships

Partnerships arise when two or more individuals carry on a business together without forming a separate legal entity. In the absence of incorporation, such arrangements are treated as general partnerships, where partners share joint liability and the partnership lacks legal personality. Unlike companies, there is no statutory limit on the number of partnerships an individual may be involved in.

- **General Partnerships** are unincorporated business arrangements between two or more individuals with joint and several liability. They are not required to file financial statements or disclose beneficial ownership, making them relatively opaque.

- **Limited Partnerships** consist of at least one general partner with unlimited liability and one or more limited partners whose liability is restricted to their capital contribution. They

[342] Approved Profit-Sharing Scheme, a Revenue-approved employee share scheme that allows employers to allocate shares to employees in a tax-efficient manner under an APSS.
[343] An Employee Share Ownership Trusts, a trust established by a company to hold shares on behalf of employees. Typically used in privatisation or restructuring scenarios, where employees are given an opportunity to acquire shares in their employer. The trust borrows funds to buy shares and then allocates them to employees over time, often funded by company contributions.
[344] Charities Regulator / Annual Report 2024 / Available from: https://www.charitiesregulator.ie/media/hrolbhm5/2024-en.pdf / p.18
[345] Charities Regulator Annual Report 2020 / Available from: https://www.charitiesregulator.ie/media/jofcsyur/final_charities-regulator-annual-report-2020.pdf / p.12

are not required to file accounts or disclose beneficial ownership unless EU rules apply,[346] and Irish authorities have limited powers to investigate or dissolve them.

- **Limited Liability Partnerships** in Ireland are currently restricted to solicitor firms and regulated by the Legal Services Regulatory Authority. They offer liability protection to partners and are subject to strict professional and financial oversight. Their limited scope and stronger regulatory framework significantly reduce their attractiveness for ML/TF abuse.

Scale of Partnerships in Ireland

As of the end of 2023, there were 2,590 LPs registered with the CRO, representing a decrease of approximately 11.5% compared to 2019, when 2,926 LPs were registered.[347] As of February 2025, a total of 439 partnerships had been authorised as LLPs, representing an increase of approximately 230% compared to April 2020, when 133 LLPs had been authorised.[348]

Threats and Vulnerabilities

Threats

The ML, TF, and PF threats to which Ireland is exposed are assessed above. Legal persons and arrangements are exposed to a range of criminal threats, particularly drug offences, fraud and extortion, cybercrime, tax crime, and illicit trade and smuggling. These structures are susceptible to exploitation by criminals, OCGs, and terrorist organisations seeking to launder the proceeds of crime or finance terrorist activities for several reasons, including creating opaque and complex ownership, operating illicit businesses under a veneer of legitimacy, creating links with foreign jurisdictions, and utilising shell companies to conceal the origin and movement of illicit funds.

[346] Limited Partnerships in Ireland are generally exempt from filing accounts or disclosing beneficial ownership, but this changes when EU rules apply. If the partnership falls under EU Anti-Money Laundering directives or the EU Accounting Directive, such as when it operates as a financial vehicle, fund, or large undertaking, it must register beneficial ownership and file financial statements.
[347] Companies Registrations Office data
[348] Legal Services Regulatory Authority data

Vulnerabilities

Vulnerability 1: Opaque and Complex Ownership Structures

The establishment of legal structures enable criminals to separate legal and natural persons.[349] Common techniques for the use of legal structures by criminals include:[350]

- Creating complex ownership and control structures using legal persons and legal arrangements,[351] including establishing ownership structure across multiple jurisdictions;
- Using intermediaries and/or nominee directors / shareholders to obscure the relationship between the beneficial owner and the assets held by the legal structure; and
- Use of offshore companies and other legal persons.

In addition, the use of multiple legal persons or arrangements within a single group structure and/or numerous bank or payments accounts, can also impair efforts by FIUs, other competent authorities, and financial institutions to identify and verify beneficial ownership, and to understand the activity of these legal persons. These efforts are further complicated where legal ownership structures and transactional activity spans numerous jurisdictions,[352] especially when jurisdictions involved do not uphold robust transparency standards or require disclosure of beneficial ownership,[353] or where nominee arrangements are in place.[354]

All legal persons are capable of being used in opaque and complex ownership structures. Some, however, are more complex. For example, SPEs are typically complex legal persons, sometimes involving ownership in offshore jurisdictions with limited disclosure laws.[355] SPEs are relatively easy to establish and can be exploited for ML due to their complex structures. While beneficial ownership obligations apply to SPEs, most are not designated persons and sit outside AML/CFT supervision, however, solicitors, external accountants and others who play an important role in the establishment and operation of SPEs are designated persons.

[349] FATF and Egmont Group / Concealment of Beneficial Ownership / Available from: https://egmontgroup.org/wp-content/uploads/2021/09/2018_Concealment_of_Beneficial_Ownership.pdf
[350] Ibid.
[351] Transparency International Ireland / Weak Links / Available from: https://transparency.ie/sites/default/files/tii_weaklinks_v6.pdf
[352] FATF and Egmont Group / Concealment of Beneficial Ownership / p.29
[353] Transparency International Ireland / Weak Links
[354] FATF / Guidance on Beneficial Ownership of Legal Persons / Available from: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Beneficial-Ownership-Legal-Persons.pdf.coredownload.pdf / p.6
[355] Transparency International Ireland / Weak Links / p.27

Following the onset of the Russia/Ukraine crisis, the Central Bank identified 66 Irish SPEs with links to Russia, 32 of which were connected to sanctioned entities, highlighting the sector's vulnerability to sanctions evasion, particularly among SPEs engaged in external financing.[356]

Case Study: Use of complex Trust and Corporate structures to obscure beneficial ownership

A trust structure was established for the son of Mr. X, a client of a UK law firm, to receive illicit funds sent from an Italian company run by Mr. X.

The scheme consisted of a Luxembourg company, which was owned by a BVI company, which in turn was owned by an Irish company. The shares of the Irish company were held in trust for Mr. X's son, by a TCSP in Jersey connected to the same UK law firm. Partners of the UK law firm were named as Directors of both the BVI and Irish companies, and a close associate of Mr. X had a power of attorney in the BVI company.

The Luxembourg company received money from the Italian company, which were shown as (fictitious) sales. Using the above scheme, there was no obvious link between the funds diverted from the Italian company and the beneficial owner of the funds.

Vulnerability 2: Misuse of Legal Person Structures to Operate Illicit Businesses

Illicit actors can use legal vehicles to act as front companies, and/or to obscure and falsify transactional and beneficial ownership information. This includes the use of intermediaries and third parties in ownership chains, the generation of false accounting and invoicing records, and methods to reduce the tax base of the entity to evade tax. These methods are more easily facilitated in environments where oversight requirements are less stringent, e.g., where entities have no mandatory audit or filing requirements. The risk of companies being used in this manner is also elevated where the underlying business type is (or is purported to be) in cash-intensive sectors, or those engaged in international trade where typologies such as trade-based ML can be committed.

[356] Central Bank / Perspectives on the Evolution of the Investment Funds Sector in Ireland / Available from: https://www.centralbank.ie/docs/default-source/publications/correspondence/general-correspondence/response-to-department-of-finance-funds-sector-2030-review.pdf?sfvrsn=f34c9d1d_4 / p.47

The EU SOCTA 2025[357] highlights that "*legal business structures are infiltrated or abused by criminal networks across almost all sectors, in all crime areas. Three types of businesses are particularly affected by criminal infiltration or abuse: construction and real estate, cash-intensive businesses (particularly hospitality), and logistics (i.e. transport and import/export companies)*".

In Ireland, this risk is partially mitigated through the Companies Act 2014 requiring that legal persons undergo an external audit. A company must appoint an external auditor unless it qualifies for an exemption, based on specific size criteria. To be eligible, the company must not exceed €7.5 million in balance sheet total, €15 million in annual turnover, and must have no more than 50 employees.[358,359] If a company meets these criteria, it is not required to submit audited financial statements, though legal persons registered with the CRO must still file unaudited financial statements to the CRO. While this exemption is intended to reduce the regulatory burden on smaller enterprises, it presents a potential vulnerability in terms of financial transparency and oversight.

Vulnerability 3: Exposure to High-Risk or Offshore Jurisdictions

All legal persons and arrangement types enable the creation of links with overseas jurisdictions, for example through beneficial ownership by non-Irish residents, or operations and investments of the legal persons having an international dimension. These can include links and exposures to high-risk jurisdictions, and those with sanctions regimes applied against them.

For example, SPEs may be exposed to high-risk jurisdictions, as of end-2021, SPEs held €37.1 billion in Russian-issued assets, the highest among Irish sectors, all through 33 Russian sponsored, non-securitisation vehicles used for external financing for Russian parent entities. This represented 8% of the non-securitisation sector. The assets and number of Russian sponsored SPEs have declined since 2016, largely due to vehicles sponsored by banks, with some unable to issue new debt after the introduction of sanctions since 2014.[360] As noted in Vulnerability 1, links to offshore jurisdictions further elevate risk.

[357] Europol / EU Serious and Organised Crime Threat Assessment, 2025 / Available from: https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf / p.27
[358] Companies Registration Office / Audit Exemption / Available from: https://cro.ie/annual-return/financial-statements-requirements/audit-exemption/
[359] The following companies are not entitled to an audit exemption: Public Limited Companies, Public Unlimited Companies and Investment Companies, A credit institution or insurance undertaking, A company referred to in the Fifth Schedule to the 2014 Act.
[360] Central Bank of Ireland / Statistical Release / Available from: https://www.centralbank.ie/docs/default-source/statistics/statistical-publications/direct-financial-links-to-russia-by-economic-sector-4-march-2022.pdf / p.2

Case Study: Offshore risk and opacity in Irish LPs

The Pandora Papers showed that significant numbers of Irish LPs' partners are based in offshore jurisdictions, often secrecy jurisdictions. This puts those operating Irish LPs beyond the reach of regulators, enforcement agencies and creditors, and increases the secrecy and opacity of the LPs' structures. This is especially so when, as is usually the case, the overseas partners are also corporate entities. The use of partners based in secrecy jurisdictions has been identified as a risk factor by the IMF.

Vulnerability 4: Verification of Information Submitted to Beneficial Ownership Registers

There is limited ability for those administering beneficial ownership registers in Ireland to verify information provided to them. For example, when a company is incorporated without the assistance of a TCSP, the CRO is responsible for the submission and processing of legal documentation. However, the CRO does not directly conduct verification or AML checks as part of this process. The CRO operates as a 'good faith' register, relying primarily on self-reported information from companies without independently verifying critical details, such as the identities and credentials of directors. This absence of proactive verification mechanisms creates a risk of the register being abused. This vulnerability is also present with the CRBOT register, and the interoperability between registers can also present difficulties in verifying information provided.

Case Study: Concentrated company registrations at a single Dublin address

In 2021, nearly 100 companies registered over just two weeks were all linked to a single residential address in a South Dublin suburb, registered by a Chinese national. Many of the companies had nonsensical names, and filings listed directors with addresses in China and mainland Europe. The same names of directors were used for multiple of these entities, however with differing addresses (sometimes in different countries). Additional investigations uncovered a separate tranche of over one hundred company registrations, which appeared to be using the addresses of legitimate businesses as the registered addresses of bogus companies.

New requirements have been introduced under Section 35 of the Companies (Corporate Enforcement Authority) Act 2021[361] to address this issue. Directors must now provide an Irish Personal Public Service Number (''PPSN'') when incorporating a company, filing an annual return, or notifying changes to directors or secretaries. The CRO also now cross-references submitted PPSNs with records maintained by the Department of Social Protection, verifying the director's name and date of birth. Although these measures have enhanced accuracy of information, the CRO's reliance on self-reported information for other aspects of company registration continues to create exposure to potential misuse. The requirement to submit PPSN information to the Irish Beneficial Ownership registers also exists under the beneficial ownership registers legal framework, i.e. S.I. 110 of 2019 (RBO Register) (as amended by S.I. 233 of 2020 (BORCFV Register)) and S.I. 194 of 2021 (CRBOT Register).

To further strengthen oversight, following the transposition of Article 10 of the AMLD6 in July 2027, Ireland's three beneficial ownership registrars will be empowered to conduct rigorous verification of data provided, including powers to carry out on-site inspections of registers for verification purposes.

Vulnerability 5: Shell Companies

As noted by the FATF, "*The use of shell companies in complex corporate structures designed to disguise beneficial ownership is a consistent and enduring technique used by criminal groups, corrupt individuals, and complicit professionals*".[362] All legal persons can be used as a shell entity, however some legal entity types (for example SPEs) can be more attractive due to their inherent features such as minimal physical presence, limited personnel, and nominal operational activity, which makes them susceptible to exploitation for illicit purposes.

Consequence

Legal Persons and Arrangements are integral to the structure and operation of the financial system, providing vehicles for ownership, control, and asset management. A substantive ML, TF, or PF incident involving these entities could undermine the transparency and integrity of financial and legal arrangements, leading to significant impacts on national interests and resulting in reputational damage to the Irish financial sector. As such, the consequence has been rated as significant.

[361] eISB / Companies (Corporate Enforcement Authority) Act 2021 / Available from: https://www.irishstatutebook.ie/eli/2021/act/48/section/35/enacted/en/html
[362] FATF and Egmont Group / Concealment of Beneficial Ownership / p.31

EU Supranational Risk Assessment

The EU Supranational Risk Assessment assessed companies and trusts in its most recent (2022) risk assessment as per the below:

Sub-Sector	TF Risk	ML Risk
Companies	Moderately Significant	Very Significant
Trusts	Moderately Significant	Significant

The EU Supranational Risk Assessment notes key vulnerabilities for companies and trusts, all of which overlap with the vulnerabilities as described by the FATF.

Horizon Scanning

This section explores emerging risks and trends, offering insights into potential future vulnerabilities within Ireland's Legal Persons and Arrangements.

EU Regulatory Developments

The upcoming EU AML Regulation and establishment of AMLA will require Ireland to enhance enforcement and align with stricter EU-wide standards. This includes improving the effectiveness of its beneficial ownership framework and corporate oversight.

The Registration of Limited Partnerships and Business Names Bill 2024

The Registration of Limited Partnerships and Business Names Bill 2024[363] is currently at an advanced stage of development. The Bill seeks to enhance the legislative framework governing LPs and business names in Ireland, replacing the LPs Act 1907 and the Registration of Business Names Act 1963.

Key proposed reforms include a new definition of LPs, mandatory five-year re-registration cycle for both LPs and business names, and the introduction of stricter registration requirements, such as demonstrating a tangible connection to the State and EEA residency criteria for at least one general partner. LPs will be required to include "limited partnership"

[363] Department of Enterprise, Tourism and Employment / General Scheme of Registration of Limited Partnerships and Business Names Bill 2024 accompanied by RIA / Available from: https://enterprise.gov.ie/en/legislation/general-scheme-registration-of-limited-partnerships-and-business-names-bill-2024.html

or “LP” in their name, and their registration certificate will state that the partnership is a business agreement without separate legal personality.

The General Scheme also provides for the establishment of a beneficial ownership register for partnerships with non-EEA links. LPs will be obliged to file annual confirmation statements and continue to submit financial statements where required. The Registrar has the authority to remove LPs from the Register where there is non-compliance, exposing all partners to general liability.

Following the publication of the General Scheme and accompanying Regulatory Impact Analysis in July 2024, the Department of Enterprise, Tourism and Employment secured Government approval to proceed with the drafting of the Bill.

The Funds Review 2030 included in its recommendations several which were specific to improving transparency of SPEs, including (i) that the new EU AML/CFT legislation be transposed as a priority, (ii) that legislation be progressed to enable the Revenue Commissioners to publish a list of SPEs availing of the section 110 regime, including the name of the entity, with the list updated at regular intervals and (iii) that the Department of Finance and the Revenue Commissioners should consider how to implement a requirement for a Legal Entity Identifier from entities availing of the section 110 designation, which should be updated annually.

Trust and Company Service Providers

This assessment builds upon Ireland's 2022 Trust or Company Service Providers Risk Assessment. Since the 2022 assessment, there have been no significant changes in the sector's overall risk scores, and findings remain consistent with those previously identified. While the ratings remain unchanged, this updated assessment incorporates refreshed data and reflects relevant developments.[364]

Executive Summary

	2022 Risk Ratings	2026 Risk Ratings
Supervised by Central Bank		
ML	Medium-Low	Low
TF	Low	Low
PF	Not Assessed	Low
Supervised by Designated Accountancy Bodies		
ML	Medium-High	Significant
TF	Medium-Low	Moderate
PF	Not Assessed	Low
Supervised by Anti-Money Laundering Compliance Unit		
ML	Medium-Low	Moderate
TF	Low	Low
PF	Not Assessed	Low

Key Insights

TCSPs play a crucial role in the formation, management, and administration of legal persons and arrangements in Ireland. Individuals and groups involved in ML, TF, and PF can exploit the following features of TCSPs to facilitate and conceal their illicit activities.

- **TCSP Operations and the Transparency of Beneficial Ownership:** TCSPs often provide services to complex structures, which can make it difficult to ascertain and gather accurate beneficial ownership information.

- **Dispersed Oversight Frameworks:** The supervisory framework for TCSPs in Ireland is divided across four distinct supervisory bodies: the Central Bank, the four DABs, the AMLCU of the Department of Justice, and the Law Society. This division of supervisory

[364] Government of Ireland / Trust or Company Service Providers Risk Assessment / Available from: https://www.amlcompliance.ie/wp-content/uploads/2022/03/TCSP-Risk-Assessment.pdf

responsibility has resulted in a fragmented oversight landscape and heightened risk of inconsistency in supervisory approach.

The risk of PF within the TCSP sector is assessed as low, given the absence of confirmed sanctions breaches in Ireland to date and the limited exposure to jurisdictions subject to PF-related sanctions, as outlined in the PF threat assessment.

Scale and Structure of the TCSP Sector in Ireland

TCSPs are defined as any person whose business it is to provide any of the following services, as set out in Section 24 of the CJA.

a. Forming companies or other bodies corporate.

b. Acting as a director or secretary of a company under an arrangement with a person other than the company.

c. Arranging for another person to act as a director or secretary of a company.

d. Acting, or arranging for a person to act, as a partner of a partnership.

e. Providing a registered office, business address, correspondence or administrative address, or other related services for a body corporate or partnership.

f. Acting, or arranging for another person to act, as a trustee of a trust.

g. Acting, or arranging for another person to act, as a nominee shareholder for a person other than a company whose securities are listed on a regulated market.

While a TCSP may provide services beyond those listed in the statutory definition, the performance of any of the defined activities brings it within the scope of a TCSP for the purposes of the CJA. Under Section 25(1)(e) of the CJA, a TCSP is classified as a “designated person’’ and is therefore subject to the full range of obligations and compliance requirements of the CJA. TCSPs are legally required to be approved or registered as relevant with the appropriate competent authority before offering services. The AMLCU supervises TCSPs whose principals are not members of a DAB, while the Central Bank oversees TCSPs that are subsidiaries of credit or financial institutions. In addition, an MoU between the

AMLCU and the Law Society of Ireland clarifies supervisory responsibilities where solicitors are involved.[365]

1. Central Bank

TCSPs supervised by the Central Bank are assessed as posing a low risk for ML, TF, and PF. These low ratings are driven by the fact that these TCSPs are:

a. Subject to the Central Bank authorisation process and risk-based supervisory regime; and

b. Part of wider groups which are also Central Bank regulated, meaning that there are often compliance expertise, frameworks and technology in place in the group which can be utilised and adapted by the TCSP to embed ML, TF, and PF control frameworks.

TCSPs supervised by the Central Bank may provide services such as company formation, directorship and nominee arrangements, registered office provision, and acting as trustees or nominee shareholders for entities other than publicly listed companies. However, the significant majority of those authorised only provide trustee or nominee services to the customers of their parent entity. Only a small number offer other TCSP services, and these are not a substantial part of their overall service offering. These firms are supervised from an AML/CFT perspective in line with the Central Bank's wider supervisory framework, as described in the Domestic Legal and Institutional Framework section of this document.

As of April 2025, the Central Bank exercised supervisory responsibility over 39 TCSPs, representing an increase of approximately 18.2% compared to July 2021, when 33 TCSPs were under its supervision.[366]

2. Designated Accountancy Bodies ("DABs")

TCSPs supervised by the DABs are assessed as posing a significant risk for ML, while posing a moderate risk for TF, and a low risk for PF. These ratings reflect the broader supervisory framework applied by DABs, where TCSP supervision is integrated into the oversight of accountancy firms and practitioners. Authorisation by DABs is not granted exclusively for TCSP activities, and DABs may not always have visibility over which members are acting as TCSPs.

[365] Anti-Money Laundering Compliance Unit / Memorandum of Understanding with the Law Society / Feb 2016
[366] Central Bank data

Four DABs, prescribed under the CJA, act as competent authorities for their members providing TCSP services. Their supervisory role is formalised through an MoU[367] with the AMLCU of the Department of Justice, which sets out the oversight and cooperation frameworks.

TCSPs supervised by the DABs offer a wide range of services, including company formation, the provision of registered office and related address services, and the acting or arranging for individuals to serve as company directors or secretaries. Services such as acting as trustees of express trusts or as nominee shareholders are less frequent.[368]

DABs primarily supervise AML compliance among their members due to accountancy being subject to AML/CFT legislation. TCSP services are generally incidental to core accountancy offerings and provided to the same client base. While DABs apply a risk-based approach and conduct inspections, the scope and depth of supervision varies across bodies. Additionally, the absence of a public register of supervised TCSPs limits transparency in the sector.

Chartered Accountants Ireland supervises the largest cohort of TCSPs, with 574 firms offering both accountancy and TCSP services, and 76 TCSP-only firms. The Association of Chartered Certified Accountants supervises 134 firms which also provide TCSP services, while the Chartered Institute of Management Accountants oversees 54 accountancy members, 18 of whom also provide TCSP services. The Association of International Accountants supervises 13 TCSP firms.

3. Anti-Money Laundering Compliance Unit, Department of Justice

TCSPs supervised by the AMLCU are assessed as posing a moderate risk for ML, while posing a low risk for TF and PF. This lower rating is driven primarily by the fact that AMLCU regulated TCSPs are subject to an authorisation process as described in Chapter 9 of the CJA, and a risk-based supervisory regime.

The AMLCU supervises all other TCSPs not otherwise covered by the Central Bank or the DABs. As of February 2025, the AMLCU supervised a total of 472 TCSPs, representing an increase of approximately 33% compared to July 2021, when 356 TCSPs were under its supervision.[369]

[367] AMLCU / Memorandum of Understanding / Available from: https://www.amlcompliance.ie/wp-content/uploads/2019/11/AMLCU-MOU-with-Accountancy-Bodies.pdf
[368] Designated Accountancy Bodies data
[369] AML Compliance Unit data

TCSPs supervised by the AMLCU provide a wide range of services, as defined in Section 24 of the CJA. While individual TCSPs may specialise in particular areas, the sector as a whole provides the full suite of services defined in the CJA. Under Section 25(1)(e), any person carrying out these activities is considered a “designated person” and is subject to the full range of AML/CFT obligations. The AMLCU, as the Competent Authority, has the power to attach conditions to authorisations under Section 90 of the CJA.

In addition to the core statutory services, aviation leasing is a significant area of activity for the sector. A number of TCSPs assist in the establishment and maintenance of SPEs in this sector, and these entities are often subject to dual AML/CFT supervision by both the AMLCU and the Central Bank, reflecting the complexity and regulatory importance of these structures.

In 2023, the AMLCU conducted 140 inspections of TCSPs to assess compliance with AML/CFT regulations. Of these, 70% of firms were found to be compliant, 15% were partially compliant, and 2% were deemed non-compliant. An additional 13% fell into the "other" category, which included cases where entities were found not to be designated persons or were suspected of operating without proper authorisation.[370] The 2023 AMLCU Annual report notes that TCSPs found to be operating without proper authorisation were subject to unannounced inspections and potential enforcement actions.

The AMLCU has the authority to issue regulatory directions under several provisions of the CJA. This includes, but is not limited to, Section 63, which empowers the competent authority to direct designated persons, including TCSPs, to take specific remedial actions where compliance deficiencies are identified. Additionally, directions may be issued under Sections 17 to 21 in the context of investigations. From January 2023 to February 2025 a total of 14 regulatory directions were issued by the AMLCU to TCSPs.[371]

4. Law Society

There is also an MoU outlining the position agreed between the Law Society and the AMLCU with regard to solicitors.[372] Under the MoU, the Law Society, as the competent authority for solicitors under the CJA, has responsibility to monitor solicitors when they provide trust and company legal services and to take measures that are reasonably necessary for the purpose of securing compliance by solicitors with Part 4 of the CJA. As noted in the memorandum, the Law Society is responsible for supervising the solicitor when they provide trust or

[370] Department of Justice / AMLCU Annual Report 2023 / Available from: https://www.amlcompliance.ie/wp-content/uploads/2024/10/AMLCU-2023-Annual-Report-Final.pdf / p.14
[371] Anti-Money Laundering Compliance Unit data
[372] Anti-Money Laundering Compliance Unit / Memorandum of Understanding with the Law Society / Feb 2016

company legal services to a TCSP. However, the MoU provides that when solicitors operate TCSPs through limited companies, the AMLCU is the competent authority. The TCSPs in such situations are corporate bodies separate from individual solicitors but which may be controlled by them, or in which they may participate. Because of the separate legal personality, a solicitor can provide the services of a TCSP through a limited company and, as such the limited company must be authorised by the Minister for Justice. LSPs pose moderate risk for ML and TF and low risk for PF as set out in the chapter on LSPs.

Threats and Vulnerabilities

Threats

The ML, TF, and PF threats to which Ireland is exposed are assessed above. TCSPs' role in forming and managing legal entities makes them attractive to criminals, OCGs, and terrorist organisations seeking to obscure beneficial ownership, move illicit funds, and legitimise unlawful activity.

Illicit actors exploit TCSPs' services, such as nominee directorships, virtual offices, and mailbox facilities, to create legal structures that conceal the identity of beneficial owners and the origin of assets. These services can also be used to establish a presence in Ireland while distancing entities from their controller.

TCSPs are also targeted for their expertise in navigating complex legal and financial systems. This knowledge can be misused to construct opaque ownership structures or facilitate ML/TF/PF through the creation of legal arrangements that disguise financial flows.

Vulnerabilities

Vulnerabilities in the TCSP sector remain largely as described in the standalone 2022 TCSP risk assessment.

Vulnerability 1: TCSP Operations and the Transparency of Beneficial Ownership

TCSPs play a central role in the formation, management, and administration of legal entities and arrangements. In fulfilling this role, TCSPs may face significant challenges in obtaining and maintaining accurate and up-to-date beneficial ownership information from their clients. These challenges are often compounded by the nature and complexity of their clients' activities. Additional difficulties may arise when onboarding clients with limited or unclear

economic activity, particularly when such entities or their beneficial owners are established in foreign jurisdictions.[373]

Moreover, the reliability of beneficial ownership information may vary depending on its source, whether it is obtained from a public registry, or directly from the client. The accuracy of such data can be especially uncertain when it is self-reported, increasing the risk of incomplete or misleading information.[374]

Criminals can use TCSPs to obtain specialist advice and skills in complex financial, business, company, and tax matters to disguise the true ownership or source of their assets. Operating through or behind a TCSP provides a veneer of legitimacy to criminal activities and, where complex structures are established, creates distance between criminal entities and their illicit wealth.[375]

In addition to establishing legal persons on behalf of clients, TCSPs, offer directorship, virtual office and mailbox services. These services allow the legal person to maintain a physical footprint in a country and can distance the legal person from other assets and activities controlled by the beneficial owner. As a result, these services are vulnerable to exploitation for the purpose of disguising the true controllers and beneficial owners of a legal person. Nominee directors and virtual offices are common features in many complex legal structures that are involved in ML.[376]

The assessment of TF related to the creation of legal entities and legal arrangements shows that terrorist organisations may have difficulty in creating such structures. Knowledge of both domestic and international regulatory and taxation rules are required to create these structures which entail a high level of specialism which can be provided by TCSPs.[377]

Ireland has established central registers to improve transparency around beneficial ownership, the RBO, the CRBOT and BORCFV. TCSPs have specific obligations under these frameworks and must register their own beneficial ownership information and verify the beneficial ownership of client entities. TCSPs must also conduct independent verification as part of their CDD obligations under the CJA to ensure accuracy. Further detail is provided in the beneficial ownership registers section.

[373] FATF / Trust and Company Service Providers / Available from: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/RBA-Trust-Company-Service-Providers.pdf.coredownload.pdf / p.17
[374] Ibid. / p.17
[375] FATF / Concealment of Beneficial Ownership / p.28
[376] Ibid. / p.8
[377] European Commission / Report from the Commission to the European Parliament and the Council / Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019SC0650&from=EN / p.131

Survey results indicate that TCSPs in Ireland consider 'complex ownership structures' (172 respondents, 69%) and 'lack of transparency in ownership' (150 respondents, 60%) as the primary risk factors contributing to the sector's vulnerability to ML, TF, and PF.

Case Study: Complexity of ownership structures created by TCSPs

A client of a TCSP in Ireland, whose beneficial owner was a billionaire national of an Asian country, was found to have highly complex structures in place. One such complex structure was based on a partnership. "X" Trustees (Ireland) Limited, a TCSP, acted on behalf of their client, the Asian billionaire, as the initial limited partner of a proposed partnership. "Y" Corporate Trustees (Mauritius) Limited, a TCSP, expressed an interest in becoming a partner in its role as trustee for "Z" Trust Limited. "Z" Trust Limited is a company limited by shares and incorporated in the British Virgin Islands. Other countries through which the client did business include Switzerland and the Cayman Islands. The sum of the values of the sampled entities of the client of the TCSP was over half a billion US dollars. The TCSP could not adequately explain the reasons for the complexity of the arrangements.

Vulnerability 2: Inconsistent Supervisory Frameworks

The effective management of ML/TF/PF risks in the TCSP sector is reliant on having effective and reliable supervision.

In Ireland, the supervisory framework for TCSPs is divided across four distinct supervisory bodies: the Central Bank, the AMLCU, the DABs (of which there are four), and the Law Society. This division of supervisory responsibility results in a fragmented supervisory landscape, and an inconsistent approach to regulatory oversight. For instance, while both the Central Bank and the AMLCU maintain and publish public registers of the TCSPs under their supervision, not all DABs currently provide an equivalent level of transparency. In addition, the absence of a publicly accessible list of supervised entities within the DAB-supervised population poses a challenge to the visibility and identification of all TCSPs in the sector.

Consequence

A significant ML, TF or PF incident involving TCSPs could undermine confidence in Ireland's corporate transparency framework and raise reputational concerns, particularly given the sector's role in enabling access to the formal financial system. However, the overall impact

on financial stability and national interests is assessed to be limited, due in part to the sector's relatively contained size and the presence of active supervisory arrangements, albeit distributed across multiple authorities. As such, the consequence has been rated as moderate.

Horizon Scanning

Strengthening AML/CFT Oversight of TCSPs Supervised by the AMLCU

A key reform of the National Recovery and Resilience Plan ("NRRP") focused on strengthening oversight of TCSPs. This included conducting at least 120 inspections and recruiting at least two additional staff within the AMLCU, including one with specialist skills in forensic accounting and the other in law, to support supervision and management of TCSPs.

Legislation establishing an administrative financial sanctions regime for the AMLCU or any relevant successor bodies is expected to enter into force by mid-2026. This regime will be introduced in line with the requirements of the 6th AML Directive (Directive (EU) 2024/1640) and will apply, at a minimum, to TCSPs that are not under the remit of the Central Bank or prescribed accountancy bodies.

Non-Profit Organisations

Executive Summary

	2019 Risk Ratings	2026 Risk Ratings
ML	Medium-Low	Low
TF	Medium-Low	Moderate
PF	Not Assessed	Low

Key Insights

This NPO risk assessment updates and replaces the section in Ireland's 2019 NRA, though the findings from this assessment remain largely consistent with those from 2019. The moderate rating for TF primarily reflects an elevated threat level within the sector. In contrast, the threats related to ML and PF have been assessed as low.

The NPO sector in Ireland is large and diverse, encompassing a wide range of entities that provide essential funding, services, and support across various areas of public interest. While the sector includes some internationally active organisations, it is predominantly domestic in nature, and a significant portion of their funding is sourced from government bodies, both at central and local levels. NPOs typically rely on regulated financial institutions, such as banks, for processing transactional activity, and the use of cash, whether for donations or disbursements, is limited. Although TF risk is potentially present in the sector, this is concentrated in a relatively small subset of NPOs, operating in higher-risk jurisdictions or engaging in activities that present elevated exposure to TF threats. In assessing the sector, a survey of charities registered with the CRA was carried out, the results of which are included in the assessment below.

The key vulnerabilities in the sector are:

- **Extended Logistical Networks:** A small cohort of Irish NPOs operating internationally, particularly in high-risk jurisdictions, face elevated TF risks due to complex logistical networks that are difficult to monitor and control.

- **Large Transitory Workforces:** The reliance on transient staff and volunteers, combined with limited financial crime training and oversight of international partners, potentially increases the sector's exposure to TF risks.

- **Access to Resources and Geographical Reach:** While most Irish NPOs use regulated financial channels, those with significant resources and operations in conflict zones may

be vulnerable to exploitation by terrorist groups, particularly where oversight is limited and/or IVTS are used.

- **Organisational Factors:** Low awareness of ML, TF, and PF risks, limited application of formal controls, and governance gaps in some NPOs contribute to sector-wide vulnerabilities, especially among newer or less regulated organisations.

The above vulnerabilities are factors which are inherent in the delivery of vital work by NPOs, which are addressed in part through domestic safeguards and adherence to international best practices and commitments. This includes active involvement in the 'Grand Bargain', a global agreement aimed at enhancing the efficiency and effectiveness of humanitarian aid.

Legislative Framework for NPOs

The Charities Act 2009

The Irish government enacted the Charities Act (2009) ("Charities Act") to define[378] and provide for the regulation of Charities, and to establish the Charities Regulatory Authority ("CRA"). Under the Charities Act, each of the following objectives shall be considered a Charitable purpose, organisations carrying out one of these purposes and meeting other legal requirements are registered and the NPOs are subject to the Act and regulation by the CRA:[379]

1. The prevention or relief of poverty or economic hardship;

2. The advancement of education;

3. The advancement of religion; and

4. Any other purpose that is of benefit to the community.[380]

Section 41 of the 2009 Act prohibits unregistered charitable organisations from carrying out any activities and unregistered organisations from misrepresenting themselves as charities in any manner. Offences under the Charities Act are subject to fines and custodial

[378] The definition of a charitable organisation is similar to jurisdictions such as England and Wales reflecting a shared legal heritage and common principles in charity law, with some divergence since the enactment of the Charities Act 2009.
[379] List of Charitable purpose as outlined in Section 3(1) of the Charities Act 2009 and Charities (Amendment) Act 2024. Under the Charities Act, a purpose shall not be regarded as a Charitable purpose unless it is of public benefit.
[380] List of 'any other purpose that is of benefit to the community' as outlined in Section 3(11) of the Charities Act 2009 and the Charities (Amendment) Act 2024 which will change the order in which these are listed and add the Advancement of Human Rights as a charitable purpose.

sentences, as set out in section 10 of the Charities Act. In 2024, the Irish government amended the Charities Act.[381] Key changes included adding the advancement of human rights as a charitable purpose (although implementation of this provision has not yet commenced), and provisions to enhance financial transparency and codifying charity trustee duties.

The addition of human rights charities to the cohort of NPOs falling within the CRA's statutory remit has brought the CRA's supervised population into broad alignment with FATF's definition of an NPO. As such, for the purpose of this risk assessment, the term NPO will refer to a charitable organisation under the CRA's statutory remit and the term NPO Sector will refer to the CRA's supervised population.

Criminal Justice (Money Laundering and Terrorist Financing) Act

NPOs are not directly subject to AML and CFT obligations under the CJA as they are not designated persons. However, NPOs may be indirectly subject to AML/CFT measures through their interactions with regulated financial institutions and professional service providers (who are designated persons), for instance through the provision of banking or legal services to NPOs. Many regulated institutions classify NPOs to be 'high-risk' client types, and Enhanced Due Diligence and ongoing monitoring therefore may be performed, with STRs being submitted where suspicious activity is identified. This oversight limits the risk in the sector for those NPOs which interact with the regulated sector.

Scale, Structure and Funding of the NPO Sector

Scale and Structure

Ireland's NPO sector is predominantly made up of a large number of small organisations, alongside a relatively small proportion of larger organisations. According to the CRA 2024 annual report,[382] 11,445 Charities are registered in Ireland, and around 68% of these report an annual income of less than €250,000. Ireland's NPO sector can be largely grouped into two main cohorts, Service NPOs and Expressive NPOs:[383]

- **Service NPOs:** These NPOs are involved in providing housing, social services, education, or health care. Some of these operate in specific geo-political contexts could

[381] Charities (Amendment) Act 2024
[382] CLS / The Charities Regulator Annual Report 2024 / Available from: https://www.charitiesregulator.ie/media/hrolbhm5/2024-en.pdf
[383] FATF / Best Practice Paper on Combating the Abuse of Non-Profit Organisations / Available from: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/BPP-combating-abuse-non-profit-organisations.pdf / p.15

be considered to pose heightened TF risks, including where these services are being provided geographically close to an active terrorist threat. Their humanitarian missions and urgent operations can also make them more vulnerable to infiltration or misuse.

- **Expressive NPOs:** These NPOs operate in facilitating activities such as community and amateur sports and recreation, arts and culture, interest representation or advocacy such as political parties, trade unions and think tanks. These organisations (which generally are domestic-facing) are registered and supervised by a number of organisations including the CRA, the Electoral Commission and Revenue.

In Ireland, entities such as schools, universities, hospitals, family resource centres, and community centres are often registered as charities with the CRA. However, many of these organisations do not fall within the FATF's definition of a NPO, or are at little or no risk for TF as these are state bodies providing services to the Irish population. These organisations are primarily regulated by sector specific authorities such as HIQA or the Department of Education. The CRA has the power to exempt an applicant from certain reporting requirements if it considers them unduly onerous given the applicant's circumstances, this is currently the case for primary schools. The legal structure of the majority of NPOs is that of company limited by guarantee, others are associations and a smaller number are trusts or established by statute.[384] MOUs between the CRA and these bodies also help ensure coordination and mitigate the risk of such organisations being misused for terrorist or other illicit purposes.

Funding

Government (both central and local) is the biggest individual source of funding to NPOs. The granting of public funds to NPOs is governed by the reporting requirements under the Department of Public Expenditure and Reform ("DPER"),[385] and NPOs applying for public funding are subject to a comprehensive due diligence process. This may include reviews of financial reports, rights of access to inspect relevant records maintained by the NPO, assessments of accounting and organisational structures, and completion of audited financial statements or annual declarations confirming compliance with funding conditions. Tax-related declarations may also be required.

[384] As addressed in the Legal Persons and Arrangements chapter statutory trusts cannot pose ML or TF risk
[385] DPER Circular 13/2014 - Management of and Accountability for Grants from Exchequer Funds Guidance Note and Reporting Requirements / Available from: https://assets.gov.ie/static/documents/dper-circular-132014-management-of-and-accountability-for-grants-from-exchequer-funds-.pdf

For the reporting period 2023 to 2024, NPOs with operations overseas (i.e. those deemed exposed to the highest level of TF risk) had a gross income of €575 million, of which €392 million (68%) came from government or local authority sources, with a further €11 million (2%) coming from other public sources. NPOs with operations in the highest risk countries[386] are even more reliant on public funding, with gross income of €304 million, of which €232 million (76%) came from the government or local authorities, and a further €5 million (2%) from other public sources.[387] In order to mitigate this heightened risk, NPOs applying for public funding are subject to a rigorous risk assessment process, which includes reviews of audited accounts, and analysis of fund flows prior to funding being provided.

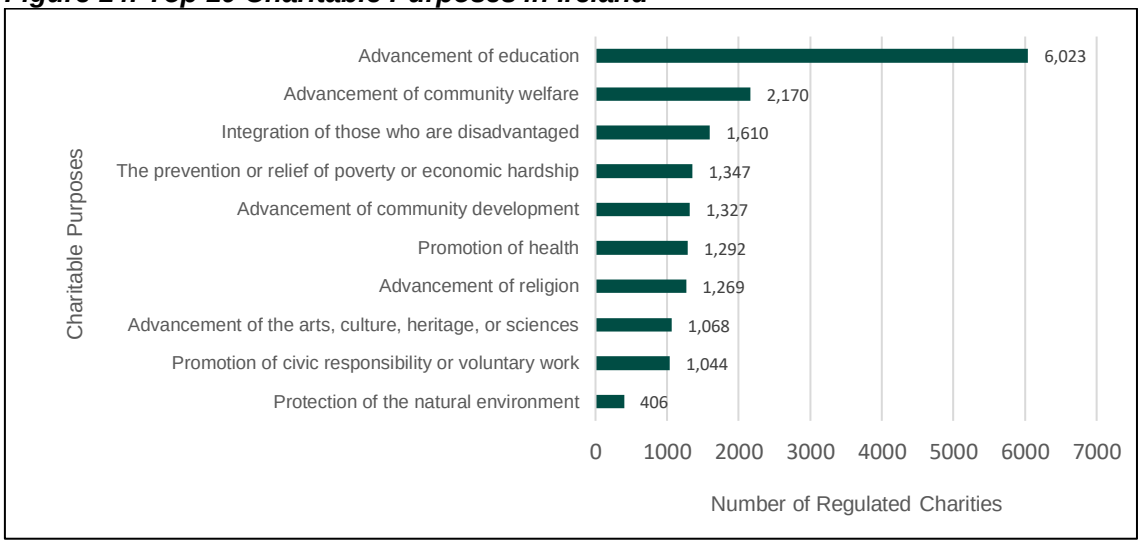
Corporate sponsors are also significant contributors to Irish NPOs. These sponsors typically have their own due diligence frameworks in place to ensure that funding is used appropriately and in alignment with their values and legal obligations. This includes measures to mitigate reputational risk and ensure compliance with ML, TF, and PF requirements, as well as to ensure that Bribery and Corruption risk is effectively managed. In addition, many public sector NPOs which are CRA registered and distribute funds are bound by the Code of Practice for the Governance of State Bodies.[388] This ethical, governance and accounting framework provides additional protections against the possibility of funds being used to assist terrorism.

Charitable Purposes

The Charities Act lists 17 Charitable purposes.[389] Figure 14 presents the distribution of the top 10 Charitable purposes in Ireland for the regulated sector; collectively, these top 10 Charitable purposes represent approximately 95% of all activities carried out by regulated NPOs in Ireland.[390]

[386] Jurisdictions identified as having heightened exposure to ML, TF, and PF risks include those classified under the FATF Black or Grey lists, designated as EU High-Risk Third Countries (HRTC), or subject to international sanctions imposed by the EU, OFAC, or the UN. Organisations operating in these jurisdictions face significantly elevated compliance challenges and require enhanced risk management measures.
[387] Data was obtained from the Full Public Register of Charities which can be downloaded from the Charities Regulator website
[388] Department of Public Expenditures, Infrastructure, Public Service Reform and Digitalisation / https://www.gov.ie/en/department-of-public-expenditure-infrastructure-public-service-reform-and-digitalisation/publications/governance/
[389] Section 3 of the Charities Act 2009
[390] Charities Regulator / Annual Report 2023 / Available from: https://www.charitiesregulator.ie/media/lrwbzoq5/annual-report-2023.pdf

Figure 14: Top 10 Charitable Purposes in Ireland*[391]



*Charities often list more than one charitable purpose.

The Charities Regulatory Authority

The CRA is the statutory body which regulates NPOs which meet the definition of a Charity in Ireland; this regulation obligates NPOs to comply with the requirements of the Charities Act. It also requires these NPOs to be subjected to the due diligence applied by the CRA during the application process and throughout their time as a registered charity. The CRA is a member of the AMLSC. NPOs applying for tax-exempt status are subject to due diligence by Revenue.

The main functions of the CRA (in relation to NPOs which meet the definition of a Charity), as stipulated by the Charities Act,[392] include:

- Maintaining a public register of NPOs
- Ensuring NPOs comply with the Charities Act
- Increasing public trust in the running of NPOs

[391] Charities Regulator Annual Report 2024, p.17
[392] Section 14(1) of the Charities Act 2009

- Publishing guidelines, codes and model documents to help NPOs and NPO trustees to comply with the Charities Act

- Ensuring NPOs are accountable to donors, beneficiaries, and the public

- Providing stakeholders including the Minister and the public, with information about regulated NPOs

Once registered, all NPOs are required[393] to submit an annual report to the CRA, which includes information on overseas transactions,[394] and some of this information – including in relation to income and trustees of the organisation – is published on the CRA register. This helps to further the CRA goal of improving public trust and transparency, and also facilitates international cooperation between oversight bodies. There are significant tax advantages to registration (subject to Revenue approval), which encourages engagement with the process. In addition to registering NPOs and maintaining a public register, the CRA reviews compliance with charity law and trustee duties in relation to the control and management of NPOs. If the CRA suspects any criminal wrongdoing by an NPO or a trustee, it is obligated to report this to An Garda Síochána, the Revenue, the CEA Director, the Competition Authority, or any other relevant authority responsible for the detection, investigation, or prosecution of offences.[395] The CRA also has statutory duty to remove an NPO from the register, including (after consultation with An Garda Síochána) where the NPO is found to be promoting purposes that are "unlawful" or "in support of terrorism or terrorist activities".[396]

Given that NPOs are not directly subject to the provisions of the CJA, the CRA has no statutory authority to regulate their ML, TF, and PF controls. However, in line with its functions as outlined in Section 14 of the Charities Act, the CRA has published guidance on countering these risks, and has facilitated AML and CFT training to the sector, which was last delivered in November 2024.

The Garda National Diversity Unit conducts additional outreach to minority communities, including at their places of worship (many of which are connected to NPOs), to build a relationship of trust with these communities, and where needed to assist in preventing individuals from becoming radicalised. As of May 2025, the CRA's ML/TF guidance published on the CRA webpage in relation to the FATF and its role has received 1,542 visitors in the

[393] Section 52 of the Charities Act 2009
[394] Since 2022, NPOs are asked to provide the total of all international transfers of funds both into and out of the State, list the countries involved, and set out the method used to transfer those funds.
[395] Section 28 of the Charities Act 2009
[396] Section 43 of the Charities Act 2009

past year. The CRA webinar on ML/TF had 115 participants and 113 visitors have subsequently viewed a recording of the webinar, and 106 visitors have downloaded the CRA guidance on ML/TF.

To enhance safeguards and support both domestic and cross-border cooperation, the CRA has established MOUs with the Revenue Commissioners and the HSE. These agreements strengthen interagency collaboration, enabling more effective oversight, enforcement, and information sharing in relation to charitable organisations. Additionally, the CRA has MOUs with the Department of Foreign Affairs and Trade and the Northern Ireland Charities Regulator, which facilitate cross-border cooperation and oversight of NPOs operating internationally.

Threats and Vulnerabilities

Threats

The ML, TF, and PF threats to which Ireland is exposed are assessed above. NPOs can be misused for TF by collecting funds from broad donor bases and distributing them to terrorist organisations, including in high-risk or conflict-zone jurisdictions. This can occur either unintentionally – where funds are diverted from legitimate purposes – or intentionally, through NPOs knowingly established to support terrorism. This threat is higher among NPOs operating in high-risk areas, using cash or opaque transfer methods, or those not subject to due diligence processes (e.g. as required when applying for and receiving public funding). Domestically, law enforcement has observed attempts by individuals linked to dissident republican activity to establish or engage with NPOs, potentially to facilitate TF or ML. This threat has been addressed in part through effective cooperation between law enforcement and the CRA.[397]

While there are potential opportunities to launder funds through the sector (such as via the granting of donations to linked organisations or the processing of refunds) the use of NPOs for ML is not considered attractive, in part due to the typically small size of donations and the limited use of cash within the sector. NPOs could potentially be used to breach PF-related sanctions, for example by providing funds, either directly or indirectly to jurisdictions of concern. However, this risk is assessed as low in the Irish context, due to the limited NPO activity in these jurisdictions. There have been no recent prosecutions for either ML or TF

[397] Department of Justice / Ireland Terrorist Financing Risk Assessment / Available from: https://www.amlcompliance.ie/wp-content/uploads/2025/04/Terrorist-Financing-Risk-Assessment.pdf / p.40

involving Ireland's NPO sector, although there have been cases in which NPO funds have been mismanaged and/or fraudulently used.

Vulnerability 1: Extended Logistical Networks

The FATF notes that NPOs can use logistical networks to collect, transfer, and deliver resources, enabling them to implement programmes across various regions with multiple partners. These extensive networks, while essential for humanitarian operations, also heighten vulnerability to TF. This is due to the involvement of numerous individuals, a wide array of activities, and significant geographic distances, which makes it more difficult to monitor and control the flow of resources. Especially for humanitarian NPOs, these networks often traverse conflict zones or areas with weak governance, increasing the risk of resource diversion or programme corruption, particularly when passing through IVTS and other less regulated sectors like unregulated money businesses.

Data published by the CRA highlights that the risk is concentrated in a small number of NPOs. Since 2022, NPOs are required to provide information about their international transfers of funds in the annual returns, and in 2021 annual returns, of the 6,565 responses provided by NPOs,[398] eight confirmed that they had transactions with High-Risk countries[399] and a further 145 (≈2%) confirmed that they had transactions with jurisdictions designated by FATF as being under increased monitoring. Data obtained through the survey issued as part of the NRA process noted that – of the 10 respondents which were operating in countries of heightened risk – eight of these distributed funds to recipient countries via bank transfers, while the remaining two provide non-financial support, such as goods, property, or services. Eight of these also reported incomes of more than €250k, four of these eight had an income of at least €5 million.

This vulnerability can also be partially mitigated through due diligence processes applied by central and local governmental bodies when NPOs apply for funding, as well as by regulated banking or payments partners through transaction monitoring processes.

[398] Charities' International Transfers of Funds 2021 – 2022 Report / Available from: https://www.charitiesregulator.ie/media/zm5lgokb/international-funds-final.pdf / p.4

[399] Jurisdictions identified as having heightened exposure to ML, TF, and PF risks include those classified under the FATF Black or Grey lists, designated as EU High-Risk Third Countries (HRTC), or subject to international sanctions imposed by the EU, OFAC, or the UN. Organisations operating in these jurisdictions face significantly elevated compliance challenges and require enhanced risk management measures.

Vulnerability 2: Large Transitory Workforces

The FATF notes that the NPO sector can rely on a transient workforce, including many volunteers. This can complicate staff scrutiny, especially for small and medium-sized NPOs, making it hard to attract and retain experts in risk assessment, compliance, and legal matters. Such personnel challenges can result in inadequate controls, increasing the risk of abuse.

In respect of the NPO sector in Ireland, as of 2022, regulated NPOs collectively employ circa 209,000 FTE.[400]

A small proportion of these organisations operate in or maintain relationships with jurisdictions identified as having heightened exposure to ML, TF, and PF risks. This operational footprint increases their vulnerability to financial crime and underscores the need for robust governance and compliance measures. The survey of the CRA supervised population carried out as part of this assessment found that within the higher-risk subset of 50 respondents, 66% (33 of 50) reported that staff receive no training on ML, TF, or PF risks or relevant Irish legislation. Only 34% (17 of 50) confirmed providing such training, underscoring a potential gap in awareness and capability among NPOs operating in elevated-risk environments.

In addition, some NPOs use local partners and agents internationally, especially in countries and regions where they lack a presence. The use of these intermediaries can increase ML, TF, and PF risk, including the risk of diversion of funds and infiltration for terrorist purposes. Where NPOs operate in jurisdictions identified as having heightened exposure, 56% (28 of 50) respondents confirmed the use of local partners or agents, or some of their international operation, and 44% (22 of 50) respondents confirmed they deal directly with the end beneficiaries. For those engaging local partners or agents, 74% conduct due diligence consistently, 12% do so occasionally, and 14% do not perform any due diligence.

Vulnerability 3: Access to Resources and Geographical Reach

The FATF notes that the NPO sector is potentially vulnerable to exploitation by terrorist groups and financiers, due to their geographical reach and access to significant resources. NPOs can have access to significant funds, may operate with cash, and may have global reach, which can be valuable to terrorist groups. As some NPOs operate in conflict areas, this can provide unique recruitment opportunities for terrorists. Additionally, high public trust

[400] Charities Regulator / Report on the Social and Economic Impact of Registered Charities in Ireland / Available from: https://www.charitiesregulator.ie/media/othbcwjd/scoeco.pdf / p.3

in NPOs means they are often subject to less scrutiny, making them attractive targets for exploitation by terrorist entities.

Based on responses to the survey, no NPO operating in jurisdictions with heightened exposure to ML, TF, and PF risks reported using cash to transfer funds. There are also strict legislative controls on the import or export of cash over €1,000,[401] which further limits the risk of the use of cash for international activities. Instead, bank transfer is the predominant method, with 40 respondents (80%) confirming its use. A further 8 respondents (16%) indicated that they provide non-financial support such as goods, property, or services. No NPOs stated that they use informal channels such as virtual assets or hawala to transfer funds. On the basis of these responses, the vast majority of transactional activity is processed through regulated channels, which helps to mitigate vulnerabilities in this higher-risk segment of the sector.

In discussions with the regulated financial sector, some noted that NPOs were considered heightened risk customer types, due to concerns over TF risks in particular. Although there are some organisations within the NPO sector that pose a heightened risk, this risk is not pervasive across the sector and so a more nuanced view of the risk posed by NPOs to regulated financial institutions would be beneficial.

Vulnerability 4: Organisational Factors

The FATF notes that organisational culture can present a vulnerability within the NPO sector. In some cases, NPOs may prioritise values or mission-driven goals over sound governance, which can lead to weak decision-making and inadequate risk management. Newly established NPOs may have less access to professional advice and structured compliance frameworks. While trust is an important principle in the sector, excessive reliance on internal or external actors without appropriate oversight can expose NPOs to misuse or abuse. This can also manifest in fundraising events such as concerts or music festivals held in aid of a cause.

For NPOs operating in jurisdictions with heightened exposure to ML, TF, and PF risks, the survey asked respondents to assess their own awareness of relevant regulations, laws, guidance, and risks. Among this group, 64% indicated they were either, “very well or well”, while 36% stated they were “somewhat informed.”

[401] Proceeds of Crime (Amendment) Act 2005, Section 20

In relation to the application of controls, approximately 38% (19) of the NPOs operating with heightened exposure have an up-to-date ML/TF risk assessment. This is aligned with the lower level of awareness of ML, TF, and PF regulations, laws, guidance and risks in general within the NPO sector in Ireland.

Consequence

As noted above, the Irish NPO sector is large, and delivers vital goods and services domestically and internationally. A substantive ML, TF or PF incident in the sector would cause considerable damage to the level of trust afforded to the sector, potentially reducing the level of donations provided and harming genuine end beneficiaries of these funds. As such, the consequence has been rated as significant.

EU Supranational Risk Assessment

The EU Supranational Risk Assessment assessed the NPO sector in its most recent (2022) risk assessment as per the below:

Institutional Funding	TF Risk	ML Risk
No	Moderately significant	Moderately significant
Yes	Lowly significant	Lowly significant

The EU Supranational Risk Assessment notes key vulnerabilities in the NPO sector relate to the below, all of which overlap with the vulnerabilities as described by the FATF. Generally, TF and ML risk scoring in this risk assessment aligns with the EU SNRA, with the due diligence performed by central and local governmental agencies acting as an effective mitigant for both TF and ML. In an Irish context, ML risk is considered to be lower than TF risks due to the limited opportunities to launder using NPOs, and the exposure of Irish NPOs – albeit within a relatively small cohort – to countries of TF concern.

Horizon Scanning

The below are new and emerging threats and vulnerabilities which may impact on the NPO sector.

<u>Crowdfunding and Social Media</u>

Crowdfunding is a mechanism for raising funds for business ventures, charitable causes and other legitimate ends, however, in jurisdictions outside of Ireland it has also been used by

terrorist groups including ISIL to raise funds[402] with limited ability to understand those who are donating through these mechanisms. Crowdfunding activities can be significantly aided through the use of social media; As of January 2023, Ireland had 4 million social media users, representing 79.8% of the total population,[403] and this is projected to increase to 5.2 million users by 2029.[404]

Crowdfunding for NPOs can pose TF risks, either because the NPO is intentionally diverting funds to a TF use, or because the funds are diverted from a legitimate use to TF purposes; identifying illicit activity on crowdfunding platforms can also be difficult due to the difficulties in verifying donors and tracing beneficiaries. Social media is widely used to amplify and generate momentum for crowdfunding campaigns, with bad actors including terrorist groups sharing access to their networks through social media, with some platforms offering features such as encryption which are attractive to these groups.

In December 2021, Ireland implemented the EU Crowdfunding Regulations 2021 (S.I. No. 702/2021) to comply with Regulation (EU) 2020/1503 which was implemented to establish an EU regulatory framework for crowdfunding service providers.

Use of Cryptocurrencies/Virtual Assets

The Giving Block, a prominent cryptocurrency donation platform, projects that $10 billion in virtual asset donations will be made globally by 2032.[405] Please see the sectoral risk assessment of Virtual Assets for a description of the ML, TF, and PF vulnerabilities associated with the sector.

Evolving Geopolitical Landscape

The global and domestic political landscape significantly impacts the NPO sector. Rising geopolitical tensions, increased economic strain, and growing polarisation can create an environment in which there is greater demand for the vital goods and services delivered by

[402] FATF / Crowdfunding for Terrorism Financing / Available from: https://www.fatf-gafi.org/en/publications/Methodsandtrends/crowdfunding-for-terrorism-financing.html / p.5
[403] Datareportal / Digital 2023: Ireland / Available from: https://datareportal.com/reports/digital-2023-ireland#:~:text=The%20state%20of%20digital%20in%20Ireland%20in%202023&text=There%20were%204.99%20million%20internet,percent%20of%20the%20total%20population
[404] Statista / Social Media and User-Generated Content / https://www.statista.com/statistics/568962/predicted-number-of-social-network-users-in-ireland/
[405] Businesswire / 2023 Annual Report on Crypto Philanthropy Reveals the Industry is on the Rise, Forecasted to Hit $10B in Crypto Donations in the Decade Ahead / Available from: https://www.businesswire.com/news/home/20230329005150/en/2023-Annual-Report-on-Crypto-Philanthropy-Reveals-the-Industry-is-on-the-Rise-Forecasted-to-Hit-%2410B-in-Crypto-Donations-in-the-Decade-Ahead

the NPO sector, as well as a greater scope and risk of funds being intentionally or unintentionally used for TF purposes.

In addition, there is an emerging trend – particularly in the US, but also in the UK, France and other European jurisdictions – of cuts to budgets for NPOs. These cuts will strain the resources of those Irish NPOs reliant on this funding and could push some NPOs to seek alternative funding sources, including from less transparent or higher-risk sources. Such a shift would increase the overall vulnerability of the sector to ML, TF, and PF threats.

Accounting Services Providers

Risk Rating

	2019 Risk Ratings	2026 Risk Ratings
ML	Medium-High	Significant
TF	Medium-High	Significant
PF	Not Assessed	Low

Profile of Sector

The accountancy sector in Ireland includes a broad range of service providers, from sole practitioners and small firms to large international accountancy networks. It also encompasses individuals offering accountancy services without formal accreditation. The supervised population is largely made up of small and micro-businesses, which deliver a variety of professional services, including accountancy and tax compliance services, payroll management, bookkeeping and insolvency support. Some ASPs also provide audit and TCSP functions. TCSP activities are assessed separately in this document.

There are four DABs which conduct supervision of their members and member firms in the sector, and supervisory collaboration among these DABs is well-established, particularly in TCSP supervision and AML reporting. Annual AML supervisory reports and registration processes are aligned across the bodies, promoting consistency and shared standard. In parallel, the AMLCU, operating under the Department of Justice, acts as the State Competent Authority for supervising ASPs who are not members of a DAB. The AMLCU also supervises TCSPs where the principals are not affiliated with any DAB.

Threats

ASPs are exposed to significant ML and TF risk due to the sector's accessibility, diversity, and the breadth of services offered. Criminals may exploit ASPs not only to lend legitimacy to illicit transactions, but also to enhance the overall credibility and respectability of illegitimate business activities. The involvement of a qualified and professional accountant can create a veneer of legitimacy that helps obscure the true nature of criminal enterprises. This can occur through services such as bookkeeping, payroll, tax advice, and the use of accountant's certificates to support falsified documentation, making illicit operations appear compliant and trustworthy to third parties. The risk is elevated in cases involving cash-intensive businesses, where criminal proceeds can be more easily co-mingled with legitimate income.

When delivered effectively and in line with the ML regulations, ASPs play a vital role in safeguarding against economic crime, however, weak or poorly implemented AML controls can be targeted by criminals. In rare but serious instances, there is also a risk of infiltration by criminal organisations, or corruption of staff within legitimate firms. ASPs that provide TCSP services face additional exposure, while those offering audit services play a key role in identifying and preventing economic crime. There has been no evidence to suggest that ASPs are being exploited for PF purposes, and the sector's exposure is therefore assessed as low. Nonetheless, continued vigilance is essential, particularly where services intersect with high-risk jurisdictions or involve complex corporate structures.

Vulnerabilities

While accountancy services, when delivered in line with legal obligations, can serve as a strong defence against economic crime, weaknesses in execution, whether accidental, negligent, or complicit, can inadvertently facilitate criminal activity. Financial distress and intimidation may be factors in cases of complicity, and once a client relationship is established, practitioners may find it difficult to disengage, even when concerns arise. This can be compounded by a reluctance to challenge long-standing clients or by a lack of formal disengagement procedures within smaller firms.

Some individuals in Ireland operate outside the regulated sector, using the title 'accountant' or 'financial advisor' without formal qualifications or oversight. These unregulated providers may unknowingly facilitate illicit activity due to limited awareness of AML/CFT obligations and risk indicators. In addition, ASPs engaged in the misuse of accounting services for illicit purposes often avoid interaction with supervisory authorities and remain disconnected from the regulated sector, further increasing the risk of misuse.

In contrast, regulated ASPs knowingly involved in illicit activity may be well-versed in regulatory requirements and ensure CDD records and related documentation are maintained to a high standard to create a façade of compliance. While such records may be falsified, their presence can complicate detection efforts and obscure the true nature of the activity.

The fragmentation of services can pose a risk. Criminals may engage different ASPs for distinct functions, such as tax advisory, payroll processing, and bookkeeping, thereby limiting each provider's visibility of the client's overall financial activity. This compartmentalisation can prevent any single firm from developing a comprehensive understanding of the client's operations, making it more difficult to identify suspicious patterns or inconsistencies. Smaller ASPs may only be engaged for specific tasks and lack access to broader financial records, impairing their ability to assess risk effectively.

Consequence

ASPs act as gatekeepers to the financial services sector. A substantive ML, TF or PF incident in the sector would have a significant impact on the financial sector and result in reputational damage to Ireland's financial services sector. As such, the consequence has been rated as significant.

Control Weaknesses

While most Irish ASPs demonstrate good compliance with AML regulations and CDD processes, control weaknesses persist in the form of gaps in awareness, oversight, or inconsistent application of procedures. These lapses are often linked to limited resourcing, particularly in smaller firms, where AML/CFT responsibilities may not be adequately supported by dedicated personnel or systems.

Between 2020 and 2024, the total volume of STRs submitted by ASPs remained consistently low, with submissions ranging from 9 to 33 reports annually. While this may be indicative of the sector's strong AML/CFT expertise, it may also be an indication of lower levels of understanding of ML red flags, given the heightened threat in the sector. Supervisory inspections by DABs have not raised concerns about under-reporting, suggesting current volumes may be proportionate to risk; however, the persistently low figures may indicate a potential weakness in detection or escalation processes and should be adequately considered during supervisory activities.

Legal Services Providers

Risk Rating

	2019 Risk Ratings	2026 Risk Ratings
ML	Not Assessed	Moderate
TF	Not Assessed	Moderate
PF	Not Assessed	Low

This chapter should be read in conjunction with the Real Estate and TCSP chapters, which contain information on risks for Legal Services Providers ("LSPs") conducting conveyancing and TCSP related activity.

Profile of Sector

The legal services market in Ireland comprises regulated providers, such as solicitors and barristers. Litigation and conveyancing remain restricted to solicitors, but commercial contracts between companies can be executed without legal representation (though solicitors are often engaged to protect the interests of the relevant parties). The industry is a mix of large and small firms, as well as a growing set of boutique firms offering specialist legal services. Solicitors are subject to AML/CFT supervision by the Law Society, which supervises approximately 2,443 firms, of which 2,046 hold client funds. Solicitors who provide trust and company legal services through a limited company are subject to authorisation and monitoring by the AMLCU within the Department of Justice. This supervisory oversight arrangement is formalised in a Memorandum of Understanding between the Law Society and the Department of Justice. In addition, there are 2,072 barristers[406] who are members of the Law Library and are supervised by the LSRA.

Threats

The responsible and compliant provision of legal services provides an effective control within the overall AML/CFT ecosystem, and in the identification and prevention of ML. However, LSPs remain attractive to criminals due to the nature and breadth of services provided, the large values which can be transacted through LSPs, and the ability of an LSP to provide apparent legitimacy to criminal activity. While client accounts are subject to strict regulatory

[406] Per the Law Library register accessed on 23rd September 2025

oversight,[407] they may be exploited for illicit purposes, including the movement of illegal funds and the fraudulent misuse of client monies by solicitors.

Vulnerabilities

Services provided by LSPs – in particular conveyancing, TCSP activities, the provision of client money accounts and complex financial transactions (including securities and fund transactions) are the most vulnerable to illegitimate use.

Client money accounts are subject to similar vulnerabilities as Retail Banking products, in that accounts enable the movement of significant funds, including internationally, although LSPs generally have strict controls on the acceptance of cash payments. Client money accounts can be used by LSPs to (knowingly or unknowingly) move significant amounts of illicit funds on behalf of criminal clients; firms with lax controls in relation to their management of client funds – including in relation to establishing source of funds – are more exposed to this vulnerability.

Providing LSP services in relation to complex transactions also poses vulnerabilities, including in situations where there are significant funds being transferred, where there are international dimensions to transactions (in particular links to jurisdictions considered to pose heightened risks), and where multiple LSPs are involved. Criminals may use multiple LSPs to complicate due diligence and obscure transactions. While most prefer a single lawyer or firm, ultra-high-net-worth individuals seeking to avoid scrutiny might engage several firms, making it harder for any one provider to detect illicit activity, especially when source of funds checks are insufficient.

While LSPs (solicitors only) are subject to ongoing, risk-based inspections by the Law Society, covering a range of compliance topics including AML/CFT controls, a persistent vulnerability remains in the form of compliance issues. Between 2020 and 2024, 49% of firms showed AML/CFT deficiencies, such as poor documentation of risk-based KYC and inadequate beneficial ownership checks. Although the rate of firms assessed as non-compliant has dropped from 9% to 1%, the continued prevalence of lower-level issues suggests weaknesses in AML implementation across the sector.

[407] Solicitors Account Regulations 2023, SI 118/2023

Table 28: Inspections and compliance rates for Solicitors (2020 – 2024)

Year	Total inspections	Compliant	Compliance issues	Non-compliant
2020	327	267 (82%)	31 (10%)	29 (9%)
2021	308	189 (61%)	99 (32%)	20 (7%)
2022	298	152 (51%)	146 (49%)	0
2023	332	134 (40%)	196 (59%)	2 (1%)
2024	342	169 (49%)	169 (49%)	4 (1%)

Under Section 45(1) of the Legal Services Regulation Act 2015, "a legal practitioner shall not hold moneys of clients unless that legal practitioner is a solicitor," subject to exceptions prescribed by regulation. The term legal practitioner includes practising solicitors (including solicitor firms) and practising barristers. However, barristers are generally not directly engaged by clients and are prohibited from handling or accessing client funds. Instead, they rely on the AML/CFT measures implemented by referring solicitors. This prohibition significantly reduces their exposure to money laundering and terrorist financing risks compared to solicitors, who routinely manage client funds and are subject to direct AML/CFT obligations.

There is no evidence of the use of LSPs for the purposes of PF, and the risk is therefore classified as low.

Consequence

LSPs play a critical role in facilitating financial and commercial transactions, as well as ensuring compliance with legal and regulatory requirements. A substantive ML, TF, or PF incident within this sector could significantly undermine the integrity of financial and legal processes, leading to reputational damage to Ireland's legal sector. As such, the consequence has been rated as very significant.

Control Weaknesses

The current legislative framework restricts the Law Society's enforcement capabilities in its role as a national AML/CFT supervisor. Unlike other competent authorities, the Law Society lacks the statutory power to impose administrative fines or pecuniary sanctions for non-compliance. This limitation weakens its enforcement arsenal.

Appendix 1: Organised & Serious Crime Branches of AGS

Table 29: Organised and Serious Crime Branches of An Garda Síochána

Organised & Serious Crime	
Branch	**Description**
Garda National Bureau of Criminal Investigation	The Garda National Bureau of Criminal Investigation ("GNBCI") comprises a number of specialised units, each addressing distinct areas of criminal activity. These include the Criminal Investigation Department for major crimes, the Serious Crime Review Team ("SCRT") also known as the Cold Case Unit which reviews historical unresolved cases or current major crime incidents with a primary aim of assisting in identifying new investigative opportunities. Other units focus on extradition, stolen vehicles, stolen arts and antiques, intellectual property violations, environmental and waste crimes, passport fraud. Additionally, the GNBCI supports international efforts in investigating genocide and war crimes, reflecting its broad and critical role in both domestic and global law enforcement.
Garda National Drugs and Organised Crime Bureau	The Garda National Drugs and Organised Crime Bureau ("GNDOCB") is a specialist unit within the OSC with responsibility for proactively targeting and investigating high-risk criminal networks primarily involved in murder, drug trafficking, firearms trafficking, armed robbery and associated money laundering.
Garda National Protective Services Bureau	The Garda National Protective Services Bureau ("GNPSB") provides advice, guidance and assistance to Gardaí investigating sexual crime, online child exploitation, domestic abuse, human trafficking, and organised prostitution. The GNPSB leads complex investigations and works closely with Government departments, State agencies, and voluntary organisations, promoting a multi-agency approach. The GNPSB also manages sex offenders, missing persons cases, and provides victim support.
Garda National Economic Crime Bureau	The Garda National Economic Crime Bureau ("GNECB") is headed by a Chief Superintendent who is also the Head of the FIU Ireland. The GNECB is responsible for investigating serious and complex economic crimes, as well as financial crimes that are of major public concern. It provides support and assistance to local and regional investigators, plays a proactive role in the prevention and detection of economic crime, and investigates all cases of foreign bribery and corruption in accordance with legislation. Additionally, the GNECB acts as a central repository for intelligence related to economic crime. The Bureau is composed of several specialised units and sections, including the Assessment Unit, Serious Economic Crime Investigation Unit, Payment Card and Counterfeit Currency Unit, Anti-Bribery

	and Corruption Unit, ML Investigation Unit, Divisional Liaison Unit and the Criminal Intelligence Office.
Financial Intelligence Unit Ireland	FIU Ireland was formally established by statute through the Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018, which inserted Chapter 3A into Part 4 of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010. FIU Ireland however was in existence prior to legislative enactment. FIU Ireland is a police based FIU and comes under the auspices of An Garda Síochána. It is resourced and financed by An Garda Síochána but has the autonomy to make operational decisions and share information. FIU Ireland carries out all of the Anti-Money Laundering Directive ("AMLD") FIU functions on behalf of the Irish State.
Garda National Immigration Bureau	The Garda National Immigration Bureau ("GNIB") is responsible for all law enforcement matters pertaining to immigration. It monitors the movement of non-Irish at all air and seaports and along the border with Northern Ireland, with a view to the prevention and detection of illegal immigration and people smuggling.
Garda National Cyber Crime Bureau	The Garda National Cyber Crime Bureau ("GNCCB") is the national Garda unit tasked with the forensic examination of computer media seized during criminal investigations. These include murders, cybercrime, online harassment, computer intrusions, child exploitation offences and any criminal investigation in which computers are seized or may contain evidential data. The unit also conducts investigations into cyber dependent crimes which are significant or complex in nature including network intrusions, data interference and attacks on websites belonging to Government departments and State bodies, institutions and corporate entities.

Table 30: Garda National Crime & Security Intelligence Service Branches of An Garda Síochána

Garda National Crime & Security Intelligence Service	
Branch	**Description**
Security & Intelligence	The Security & Intelligence section identifies and analyses threats to the State from terrorism and organised crime. It is divided into two units focused on intelligence gathering in each area and supports operational teams by providing actionable leads. It also serves as the central contact point for international cooperation with law enforcement and intelligence agencies in combating terrorism and organised crime.
Special Detective Unit	The Special Detective Unit ("SDU") is responsible for the investigation of threats to the security of the State and the monitoring of persons who pose a security threat at a national and international level.
Liaison & Protection	The Liaison & Protection Unit is responsible for the protective security of the State and its institutions. It serves as the central hub for secure communications with external agencies, housing both the Interpol National Central Bureau and the Europol National Unit. The unit also manages Ireland's participation in the Schengen Information System, coordinates Garda Liaison Officers posted abroad, supports EU Council working groups, and holds an administrative role in the Witness Security Programme.

Appendix 2: Legislative & Regulatory Framework for Legal Persons

Table 31: Breakdown of the Legal Persons and Arrangements Framework

Legal Structure	Legal Framework	Beneficial Ownership Registry	Supervisory Authority / Registrar	Mandatory Audit Requirement
Companies				
Private Company Limited by Shares (LTD)	Companies Act 2014	Register of Beneficial Owners (RBO)	Companies Registration Office (CRO) / (CEA)	Yes (unless eligible for audit exemption) (excluding PLCs who are required to complete an audit)
DAC Limited by Shares				
DAC Limited by Guarantee				
Companies Limited by Guarantee (“CLG”)				
Unlimited Companies				
Public Limited Company (‘‘PLCs’’)				
EEIGs	EEIG Regulations 1989	n/a	CRO	No
Industrial and Provident Societies	Industrial and Provident Societies Act 1893	Register of Beneficial Owners (RBO)	Registrar of Friendly Societies (RFS)	Yes (unless eligible for audit exemption)
Fund Sector Legal Structures				
Investment Companies	Companies Act 2014	Register of Beneficial Owners (RBO)	Central Bank (if regulated) / CRO	Yes
Unit Trusts	Unit Trusts Act 1990	BORCFV	Central Bank	Yes
ILPs	Investment Limited Partnerships Act 1994 (as amended by 2020 Act)	BORCFV	Central Bank	Yes

Legal Structure	Legal Framework	Beneficial Ownership Registry	Supervisory Authority / Registrar	Mandatory Audit Requirement
ICAVs	Irish Collective Asset-management Vehicles Act 2015	BORCFV	Central Bank	Yes
CCFs	Investment Funds, Companies and Miscellaneous Provisions Act 2005	BORCFV	Central Bank	Yes
Special Purpose Entities (SPEs)				
FVCs	Companies Act 2014 / ECB regulation ECB/2013/40	RBO (if a company)	CRO / CEA / Statistical Reporting to Central Bank	Yes (unless eligible for audit exemption)[408]
Non-securitisation SPEs (also referred to as "Other SPEs")	Companies Act 2014	RBO (if a company)	CRO / CEA	Yes (unless eligible for audit exemption)[409]
Express Trusts				
Welfare and Community Trusts	Taxes Consolidation Act 1997	CRBOT	Revenue Commissioners	No
Pension Purpose Trusts	Pensions Act 1990 and Taxes Consolidation Act 1997	n/a	Pensions Authority / Revenue Commissioners	Yes (for approved occupational pension schemes), No (for approved retirement funds)
Employee Share Schemes	Taxes Consolidation Act 1997, Companies Act 2014 (if company)	n/a	Revenue Commissioners, CRO (if company)	No
Charitable Trusts	Charities Act 2009	CRBOT	Charities Regulator	No

[408] Companies Registration Office / Audit Exemption / Available from: https://cro.ie/annual-return/financial-statements-requirements/audit-exemption/
[409] Ibid.

Legal Structure	Legal Framework	Beneficial Ownership Registry	Supervisory Authority / Registrar	Mandatory Audit Requirement
Express Trusts (Other)	Trusts Act 1893 (as amended)	CRBOT	Revenue Commissioners	No
Partnerships				
General Partnerships	Partnership Act 1890 / EU(Qualifying Partnerships: Accounting and Auditing) Regulations, 2019	n/a	CRO (If a general partnership operates under a business name that is not the names of the partners, it must register that name only with the CRO)	A general partnership, all of the members of which are: (i) limited companies (being any type of company the liability of whose members is limited), (ii) designated ULCs, (iii) partnerships other than LPs, all of the members of which are limited companies or designated ULCs, (iv) LPs, all of the general partners of which are limited companies or designated ULCs, or (v) partnerships, including LPs, the direct or indirect members of which include any combination of undertakings referred to in (i) to (iv), such that the ultimate beneficial owners of the partnership enjoy the protection of limited liability must file returns and audited accounts.
LPs	LP Act 1907 / EU (Qualifying Partnerships: Accounting and Auditing) Regulations, 2019	n/a	CRO	A LP, all of the general partners of which are: (i) limited companies, (ii) designated ULCs, (iii) partnerships other than LPs , all of the members of

Legal Structure	Legal Framework	Beneficial Ownership Registry	Supervisory Authority / Registrar	Mandatory Audit Requirement
				which are limited companies or designated ULCs, (iv) LPs limited partnerships, all of the general partners of which are limited companies or designated ULCs, or (v) partnerships, including LPs , the direct or indirect members of which include any combination of undertakings referred to in (i) to (iv), such that the ultimate beneficial owners of the partnership enjoy the protection of limited liability. A "designated ULC" is a private unlimited company which is not exempt from the requirement to annex its financial statements to its annual return pursuant to Section 1274 of the Companies Act, 2014. This will inter alia include an unlimited company with a limited liability parent. The "ultimate beneficial owner" of a partnership or other undertaking is the natural person or persons who ultimately own or control, directly or indirectly, that partnership or

Legal Structure	Legal Framework	Beneficial Ownership Registry	Supervisory Authority / Registrar	Mandatory Audit Requirement
				undertaking. must prepare and file audited accounts
Limited Liability partnerships (including at least one solicitor partner)	Legal Services Regulation Act 2015	RBO	Legal Services Regulatory Authority	There is no legal requirement for LLPs to prepare audited financial statements. The LSRA retains the authority to request documentation that may include financial records if deemed appropriate.
Limited Liability partnerships (including at least one solicitor partner)	Legal Services Regulation Act 2015	RBO	Law Society	Solicitors Accounts Regulations 2023 (S.I. No. 118 of 2023) Solicitors are required to: -Maintain proper accounting records for at least the current and previous financial years. -Prepare balancing statements for client accounts every three months (previously every six months), reconciling actual balances with what should be held -Maintain a register of money held on joint deposit and a register of undertakings. Solicitors must engage a Reporting Accountant to: -Independently examine the firm's compliance with the Solicitors Accounts Regulations.

Legal Structure	Legal Framework	Beneficial Ownership Registry	Supervisory Authority / Registrar	Mandatory Audit Requirement
				-Submit a Reporting Accountant's Report to the Law Society, covering compliance with Parts II–IV of the regulations. -Include in the report a list of client ledger balances outstanding for two years or more, with explanations and actions taken to resolve them -The accountant must carry out sample-based testing and follow guidance from their professional accountancy body, as outlined in the official reporting template

Companies

Companies Act 2014

In Ireland, Companies are subject to the requirements of the Companies Act 2014. This legislation sets out the requirements relating to the incorporation of all companies, including private companies limited by shares, CLG companies limited by guarantee, Designated Activity Company (‘‘DACs’’), unlimited companies, and public limited companies.

The Companies Act 2014 permits one or more individuals to form a private company for any lawful purpose by subscribing to a constitution. A private company is allowed a maximum of 149 members, whereas there is no membership limit for public companies.

With the exception of Private Company Limited by Shares, all company types must appoint one secretary and at least two directors. All company officers are subject to extensive legal responsibilities as defined in the Companies Act 2014.

Types of Company Structures in Ireland

Private Company Limited by Shares

An LTD is a company registered under Part 2 of the Companies Act 2014. An LTD company has the contractual capacity of a natural person. It does not have stated objects and can undertake any activity. It has limited liability and a share capital. The company may be incorporated with a single director if desired. An LTD company must have a company secretary, and where the company has only one director, that person cannot also act as the secretary.

Companies Limited by Guarantee

CLGs, governed by Part 18 of the Companies Act 2014, do not have share capital and are typically used by not-for-profit organisations, owner-managed companies, and charities.

Unlimited Companies

Part 19 of the Companies Act 2014 governs Unlimited Companies, which can be either private or public. Private unlimited companies are required to have a share capital, while public unlimited companies may operate without share capital. Private unlimited companies are exempt from filing financial statements with the CRO, unless all members are limited.

Designated Activity Companies

There are two types of DACs:

1. **DAC Limited by Shares:** Functions similarly to an LTD but with a more specific purpose defined in its constitution. It can only engage in activities outlined in the constitution, and it has share capital. The liability of shareholders is limited to the unpaid amount on their shares.

2. **DAC Limited by Guarantee:** Unlike the DAC limited by shares, this type does not have share capital. Instead, it has members who agree to guarantee a specified amount to the company if it is wound up.

Public Limited Companies: Governed by Part 17 of the Companies Act 2014, PLCs can also include Societas Europaea and investment companies, which are specifically regulated under Part 24.

European Economic Interest Groupings: Unlike other company types, EEIGs are not registered under the Companies Act 2014, but are governed by the European Communities (European Economic Interest Groupings) Regulations 1989. They require members from at least two EU states and are not permitted to invite public investment. EEIGs do not file financial statements with the CRO.

Special Purpose Entities

Irish SPEs are broadly categorised into two types:

- **Securitisation SPEs** (also known as Financial Vehicle Corporations or FVCs) and;

- **Non-securitisation SPEs** (also referred to as “Other SPEs”)

1. Securitisation SPEs

Securitisation SPEs are used to convert illiquid assets, such as loans or mortgages, into tradable securities. The process involves transferring a pool of assets from the originator to the SPE, which then issues debt securities backed by the cashflows from those assets. Investors purchase these securities, receive regular interest payments, and bear the associated credit risk. These structures often use ‘tranching’ to offer different risk-return profiles to a variety of investors, enhancing marketability and capital efficiency for the

originator.[410] Securitisation SPEs in Ireland are governed by an ECB regulation ECB/2013/40 for statistical purposes and must report quarterly balance sheet data to the Central Bank.

Table 32: Common securitisation SPEs' business models[411]

Business Models	Securitisation SPE Activity Description
Residential Mortgage-Backed Securities	Securities backed by cashflow resulting from mortgage loans secured on residential properties.
Commercial Mortgage-Backed Securities	Securities backed by cashflow resulting from mortgage loans that have been secured on commercial properties.
Aircraft Asset Backed Securities ("ABS")	The securitisation vehicle purchases aircraft (normally sold to it by an aircraft leasing company known as an operating lessor) and financed through the issuance of debt instruments to the market. Returns to investors are primarily based on rental income on the aircraft to airlines and disposals of aircraft.
Aircraft Lease Portfolio Securitisation	A portfolio securitisation relies on a diversified portfolio of aircraft on operating leases to a number of airlines, based on the existence of a worldwide aircraft leasing market and the projected residual values of the aircraft in the portfolio.
Lease Securitisation	Vehicles where the primary assets are lease agreements, typically on aircraft or other operating equipment, including EETC (Enhanced Equipment Trust Certificate) and Portfolio Securitisation.
Aircraft Enhanced Equipment Trust Certification	An EETC securitisation enhances the creditworthiness of traditional equipment trust certificates secured by lease receivables and the leased aircraft.

2. Non-Securitisation SPEs

Non-securitisation SPEs perform a broader range of financial functions. These entities may issue debt, act as intra-group financing vehicles, or to a lesser extent serve as cash conduits.

[410] Central Bank of Ireland / Economic Letter / Available from: https://www.centralbank.ie/docs/default-source/publications/economic-letters/vol-2018-no-11-shining-a-light-on-special-purpose-entities-in-ireland-(golden-and-hughes).pdf

[411] Central Bank of Ireland / New Research on Shadow Banking and Special Purpose Entities published / Available from: https://www.centralbank.ie/docs/default-source/publications/economic-letters/vol-2018-no-11-shining-a-light-on-special-purpose-entities-in-ireland-(golden-and-hughes).pdf?sfvrsn=4

Table 33: Common non-securitisation SPEs business models[412]

Business Models	Non-Securitisation SPE Activity Description
External Financing	Funding obtained from external sources furthered as a loan to the parent.
Loan Origination	Funding obtained from the parent and furthered to external sources.
Intra-Group Financing	Loan funding from, and to, inter-group companies.
Holding Company	A vehicle set up to hold the equity of a company, or group of companies.
Financial Leasing	Engaged in lease-in lease-out agreements or as a financial intermediary in a chain of vehicles in which the end vehicle is involved in the leasing of equipment or fixed assets.
Operational Leasing	Hold fixed assets such as plant and machinery for the purposes of leasing them out.
Fund-Linked Asset Management	Linked to investment funds/firms, which hold debt, equity, loans, or other financial assets with the goal of capital appreciation, interest or dividend income.

Express Trusts

Express trusts in Ireland are typically established through the services of professional trustees, such as solicitors, accountants, or TCSPs, all of whom are designated persons under the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, and therefore subject to AML/CFT obligations. Express trusts may, however, also be created and administered by non-professionals. Trusts are required to be registered with CRBOT, administered by Revenue in Ireland. Express trusts trustees are verified by the CROBOT which cross-references submitted PPSNs with records maintained by the Department of Social Protection, verifying the Trustees name and date of birth. Express trusts are utilised for a broad range of purposes, as set out below.

1. Welfare and Community Trusts

Welfare and community trusts include trusts established to govern amateur sports clubs, including those recognised as approved bodies or persons granted exemptions from income or corporation tax under Section 235 of the Taxes Consolidation Act 1997, but which are not registered with the CRA. As these trusts are not registered with the CRA, they are not subject to the same level of regulatory scrutiny as registered charities. However, trusts benefiting

[412] Ibid.

from Section 235 tax exemptions are subject to Revenue Commissioners' oversight, which imposes obligations, including the submission of an application to Revenue, which demonstrates that the trust must be: (1) member controlled and owned and not for profit; and (2) legally established in the State and have its centre of management and control therein. In addition, most of its trustees/directors/officers must be resident within the State. Welfare and Community Trusts created to hold the assets of an approved sports body under Section 235 of the Tax Consolidation Act 1997 must register with the CRBOT.

2. Pension Trusts

Pension trusts include:

- **Approved Occupational Pension Schemes:** These are tax-advantaged pension schemes set up by employers for the benefit of their employees. They must be approved by the Revenue Commissioners to receive tax benefits. Approved Occupational Pension Schemes can be Defined Benefit, Defined Contribution, or Hybrid schemes, offering tax relief on contributions, tax-free growth, and structured retirement benefits. These schemes are generally structured as trusts, managed by trustees, and must comply with the Pensions Act 1990. The Pensions Authority supervises compliance with the requirements of the Pensions Act by trustees of occupational pension schemes.

- **Approved Retirement Funds:** ARFs are tax-approved investment vehicles that allow individuals to access and invest their pension savings after retirement, while also drawing an income. They must comply with Irish tax law (Tax Consolidations Act 1997) and be approved by the Revenue Commissioners.

The pension trust sub-sector has a lower inherent level of ML, TF, and PF risk, as – due to the longer-term nature of these investment products – they are not typically attractive vehicles for illicit finance. In addition, pension trusts are supported by strong deterrence measures and controls that have proven effective in mitigating the risks of ML/TF/PF. These measures are grounded in legislation and regulatory oversight, primarily through the Pensions Act 1990 and the supervision of the Pensions Authority.[413] The Authority is responsible for ensuring compliance with the Pensions Act, overseeing that trustees of occupational pension schemes and employers meet their legal obligations. It carries out investigations into suspected breaches, conducts on-site inspections and compliance audits, and initiates prosecutions or other enforcement actions when violations are identified.

[413] The Pensions Authority / Code of Practice for trustees of occupational pension schemes and trust retirement annuity contracts / Available from: https://pensionsauthority.ie/wp-content/uploads/2023/06/code_of_practice_for_trustees.pdf

Revenue approval is also required for a pension scheme to be granted tax-exempt status when established as a trust, including schemes set up for individual employees or company directors. Pension trusts are outside the scope of entities obligated to register with the CRBOT.[414]

3. Employee Share Schemes

Employee share schemes include:

- **Approved Profit-sharing Schemes or Employee Share Ownership Trusts:** These schemes enable companies to share profits with employees through company shares. Approved Profit-sharing Schemes ("APSSs") must be approved by the Revenue Commissioners and comply with the relevant provisions of the Taxes Consolidation Act 1997.

- **Trusts for Restricted Shares:** These trusts are used by companies to manage and distribute shares to employees or stakeholders, particularly in ESOPs. They impose restrictions on the sale or transfer of shares and are governed by a combination of trust, company, and tax law.

Although employee share schemes do not fall within the scope of entities required to register with the CRBOT, they must comply with the Taxes Consolidation Act 1997 and are subject to approval by the Irish Revenue Commissioners, which requires trustees to be subjected to detailed and ongoing reporting obligations. Funding of employee share schemes is typically provided by the employer or parent company, and where employee contributions are involved, they are usually processed through payroll deductions. Participation is limited to eligible employees, and shares allocated under APSSs must be held in trust for a minimum period to qualify for tax advantages. Collectively, these structural safeguards contribute to a well-controlled environment with minimal exposure to ML, TF or PF risks.

4. Charitable Trusts

For the purposes of this assessment charitable trusts are defined as those trusts supervised by the CRA. An example of such a trust is the Haemophilia HIV Trust (the HHT), which was established by trust deed in November 1989. The HHT was established to provide basic financial assistance for haemophiliacs who received infected blood products.[415]

[414] Revenue / Trusts required to register and certain exemptions / https://www.revenue.ie/en/crbot/trusts-that-must-register/excluded-arrangements.aspx
[415] Tax and Duty Manual / Payments by Haemophilia HIV Trust - Exemption from Income Tax / Available from: https://www.revenue.ie/en/tax-professionals/tdm/income-tax-capital-gains-tax-corporation-tax/part-07/07-01-04.pdf

When evaluating charitable trusts, deterrence measures and controls are in place, reasonably mitigating the risks of ML, TF, and PF. For example, the CRA oversees compliance with the Charities Act 2009 and has a range of powers under this Act, including the authority to appoint inspectors.

In the case of the HHT, ML and TF risk is more limited. Payments to beneficiaries are relatively modest, with beneficiaries typically receiving an initial lump sum followed by monthly payments.[416] Beneficiaries of the Trust are limited to haemophiliacs who received infected blood products in the State of Ireland, as well as their spouses/civil partners, parents, children, or other dependents of such individuals should the victim be deceased. Funding of the Trust is also entirely provided by the Irish Government (initially funded by a government grant of €1.26 million, the HHT is also supported by income generated from the investment of these funds).[417] While the CRBOT mandates registration for charitable trusts, this requirement does not extend to the HHT.[418]

Express Trusts (Other)

An express trust is defined under the EU (Anti-Money Laundering: Beneficial Ownership of Trusts) Regulations 2021 as a trust that is explicitly established through a deed or other written declaration. Examples of Express Trusts include private family trusts, along with other Express Trusts encountered in finance and commercial transactions, such as security trust arrangements, declarations of trust in respect of shares, and benefit trusts. These trusts are specifically established through written deeds or declarations and are subject to the provisions outlined in the 2021 Regulations.

For the purposes of the Irish beneficial ownership framework, an Express Trust is one where the trustees are either resident in Ireland or the trust is otherwise administered in Ireland (although some exemptions apply).[419]

[416] For example: (a) a lump sum of €5,000 followed by 30 monthly payments of €120, or (b) a lump sum of €3,000 followed by 30 monthly payments of €200.
[417] Tax and Duty Manual / Payments by Haemophilia HIV Trust - Exemption from Income Tax / Available from: https://www.revenue.ie/en/tax-professionals/tdm/income-tax-capital-gains-tax-corporation-tax/part-07/07-01-04.pdf
[418] Revenue / Excluded Arrangements / Available from: https://www.revenue.ie/en/crbot/trusts-that-must-register/excluded-arrangements.aspx
[419] Where the trustee (in its capacity as the trustee of the express trust): enters into a business relationship in Ireland; or acquires Irish real estate in the trusts name.

Partnerships

Types of Partnerships in Ireland

1. General Partnerships

Governed by the Partnership Act 1890, these partnerships impose joint liability on partners for business debts and obligations. They are typically governed internally by a partnership agreement, although this is not legally required. Where General Partnerships operate under different names from those of the individual partners, they are required to register that business name with the CRO. In addition, General Partnerships are required to submit an annual return to Revenue, containing the partnership's income and capital gains for the relevant year. However, unlike companies, General Partnerships are not obligated to file annual returns or financial statements with the CRO.

2. Limited Partnerships

Regulated by the LPs Act 1907, these structures allow for partners with limited liability, subject to registration with the CRO. Each LP must have at least one general partner with unlimited liability. Limited partners must contribute capital and are restricted from participating in management to maintain their limited liability status. LPs are not required to file accounts (except in the limited circumstances in which the EU Directive discussed in Section 2 applies), nor their constitutional arrangements or their true beneficial owners or controllers if these are not the partners (for example the majority shareholder of a corporate general partner). In Ireland, there is no power to investigate LPs, in contrast to the power to investigate ILPs or companies. Also, there is no power to compulsorily dissolve a LP which has been used in wrongdoing.

3. Limited Liability Partnerships

LLPs are currently restricted to partnerships of solicitors. Authorised LLPs offer liability protection for individual partners against debts and obligations of the LLP or actions of other partners. The regulatory framework was implemented in late 2019, with the LSRA overseeing authorisations. While provisions exist to allow legal partnerships involving barristers, these have not yet commenced.

Appendix 3: Table of Risk Ratings

Table 34

Financial Services		
	2019 Risk Ratings	**2026 Risk Ratings**
Retail Banking		
Traditional Retail Banks		
ML	High	Very Significant
TF	High	Very Significant
PF	Not Assessed	Low
Digital Banks		
ML	Not Assessed	Very Significant
TF	Not Assessed	Very Significant
PF	Not Assessed	Low
Credit Unions		
ML	Medium-Low	Moderate
TF	Medium-Low	Moderate
PF	Not Assessed	Low
Non-Retail Banking		
Higher Risk Business Activities		
ML	Not Assessed	Significant
TF	Not Assessed	Significant
PF	Not Assessed	Low
Asset Finance		
ML	Not Assessed	Low
TF	Not Assessed	Low
PF	Not Assessed	Low
Securities Transactions		
ML	Not Assessed	Moderate
TF	Not Assessed	Low
PF	Not Assessed	Low
Depositary Services		
ML	Not Assessed	Moderate
TF	Not Assessed	Low

PF	Not Assessed	Low
Covered Banks		
ML	Not Assessed	Low
TF	Not Assessed	Low
PF	Not Assessed	Low
Funds		
Investment Funds		
ML	Medium-High	Significant
TF	Medium-High	Moderate
PF	Not Assessed	Low
Funds Management Companies		
ML	Medium-Low	Significant
TF	Medium-Low	Moderate
PF	Not Assessed	Low
Funds Administrators		
ML	Medium-High	Significant
TF	Medium-High	Moderate
PF	Not Assessed	Low
Funds Depositories		
ML	Medium-High	Significant
TF	Medium-High	Moderate
PF	Not Assessed	Low
Crypto-Assets		
ML	Medium-High	Very Significant
TF	Medium-High	Very Significant
PF	Not Assessed	Low
Payment Institutions and E-Money Institutions		
E-Money Institutions		
ML	Not Assessed	Very Significant
TF	Not Assessed	Significant
PF	Not Assessed	Low
Money Remittance Firms		
ML	High	Very Significant
TF	High	Very Significant

PF	Not Assessed	Low
Payment Institutions (PIs) (other than Money Remittance Firms)		
ML	Medium-Low	Moderate
TF	Medium-Low	Moderate
PF	Not Assessed	Low
Retail Credit Firms		
ML	Not Assessed	Low
TF	Not Assessed	Low
PF	Not Assessed	Low
Bureaux de Change		
ML	High	Significant
TF	High	Moderate
PF	Not Assessed	Low
Life Insurance		
ML	Medium-Low	Moderate
TF	Medium-Low	Low
PF	Not Assessed	Low
MiFID Investment Firms		
ML	Not Assessed	Moderate
TF	Not Assessed	Low
PF	Not Assessed	Low
MiFID Markets Firms		
ML	Not Assessed	Moderate
TF	Not Assessed	Low
PF	Not Assessed	Low
Retail Intermediaries		
ML	Not Assessed	Low
TF	Not Assessed	Low
PF	Not Assessed	Low
High-Cost Credit Providers		
ML	Not Assessed	Low
TF	Not Assessed	Low
PF	Not Assessed	Low

**There were no sub-sector ratings in the 2019 NRA assessment of Non-Retail Banking; The non-Retail Banking sector overall was assessed as medium-high for ML/TF.*

Non-Financial Services		
	2019 Risk Ratings	**2026 Risk Ratings**
Real Estate		
Real Estate Assets		
ML	Not Assessed	Significant
TF	Not Assessed	Moderate
PF	Not Assessed	Low
Property Service Providers		
ML	Medium-Low	Moderate
TF	Medium-Low	Moderate
PF	Not Assessed	Low
Legal Services		
ML	Medium – High*	Significant
TF	Medium – High*	Moderate
PF	Not Assessed	Low
	2018/2019 Risk Ratings*	**2026 Risk Ratings**
Gambling Service Providers		
Retail Bookmakers		
ML	Medium-Low	Moderate
TF	Medium-Low	Low
PF	Not Assessed	Low
On-course Bookmakers		
ML	Medium-Low	Moderate
TF	Medium-Low	Low
PF	Not Assessed	Low
Remote Bookmakers (Betting Intermediaries and Exchanges)		
ML	Medium-Low	Significant
TF	Medium-Low	Low
PF	Not Assessed	Low

Private Members' Clubs (PMC)		
ML	Medium-High	Significant
TF	Medium-High	Low
PF	Not Assessed	Low
National Lottery, Local Lotteries, and Bingo Operators		
ML	Low/Medium-Low	Moderate
TF	Not Assessed	Moderate
PF	Not Assessed	Low
The Tote (both Horse Racing Ireland ("HRI") and Greyhound Racing Ireland ("GRI")		
ML	Medium-Low	Low
TF	Medium-Low	Low
PF	Not Assessed	Low
	2019 Risk Ratings	**2026 Risk Ratings**
High Value Goods Dealers		
ML	Medium-High	Significant
TF	Medium-High	Significant
PF	Not Assessed	Low
Legal Persons and Arrangements		
Companies		
ML	Medium-High	Significant
TF	Medium-High	Moderate
PF	Not Assessed	Low
Special Purpose Entities (SPEs) – SPE Securitisation		
ML	Medium-High	Significant
TF	Medium-Low	Moderate
PF	Not Assessed	Low
Special Purpose Entities (SPEs) – SPE Non-Securitisation		
ML	High	Very Significant
TF	Medium-Low	Moderate
PF	Not Assessed	Low
Express Trusts - Welfare and Community Trusts		
ML	Low	Low

TF	Low	Low
PF	Not Assessed	Low
Express Trusts - Pension Purpose Trusts		
ML	Low	Low
TF	Low	Low
PF	Not Assessed	Low
Express Trusts - Employee Share Schemes		
ML	Low	Low
TF	Low	Low
PF	Not Assessed	Low
Express Trusts - Charitable Trusts[420]		
ML	Medium-Low	Moderate
TF	Medium-Low	Moderate
PF	Not Assessed	Low
Express Trusts - Express Trusts (Other)		
ML	Medium-Low	Moderate
TF	Medium-Low	Moderate
PF	Not Assessed	Low
Partnerships		
ML	Medium-Low	Moderate
TF	Low	Low
PF	Not Assessed	Low
	2022 Risk Ratings	**2026 Risk Ratings**
Trust and Company Service Providers		
Supervised by Central Bank		
ML	Medium-Low	Low
TF	Low	Low
PF	Not Assessed	Low
Supervised by Designated Accountancy Bodies		
ML	Medium-High	Significant
TF	Medium-Low	Moderate

[420] As defined in Section 2 of the Charities Act 2009

PF	Not Assessed	Low
Supervised by Anti-Money Laundering Compliance Unit		
ML	Medium-Low	Moderate
TF	Low	Low
PF	Not Assessed	Low
	2019 Risk Ratings	**2026 Risk Ratings**
Non-Profit Organisations		
ML	Medium-Low	Low
TF	Medium-Low	Moderate
PF	Not Assessed	Low
Accounting Service Providers		
ML	Medium-High	Significant
TF	Medium-High	Significant
PF	Not Assessed	Low
Legal Services Providers		
ML	Not Assessed	Moderate
TF	Not Assessed	Moderate
PF	Not Assessed	Low

*The gambling industry was assessed in 2018, excluding PMCs. However, PMCs were evaluated in the 2019 NRA, and the relevant ratings have been assigned accordingly.

**The National Lottery and Bingo Operators are assessed as being low risk for ML, TF, and PF.

Intentionally left blank

An Roinn Airgeadais
Department of Finance

Tithe an Rialtais, Sráid Mhuirfean Uacht,
Baile Átha Cliath 2, D02 R583, Éire
Government Buildings, Upper Merrion Street,
Dublin 2, D02 R583, Ireland
T: +353 1 676 7571 | @IRLDeptFinance
www.gov.ie/finance