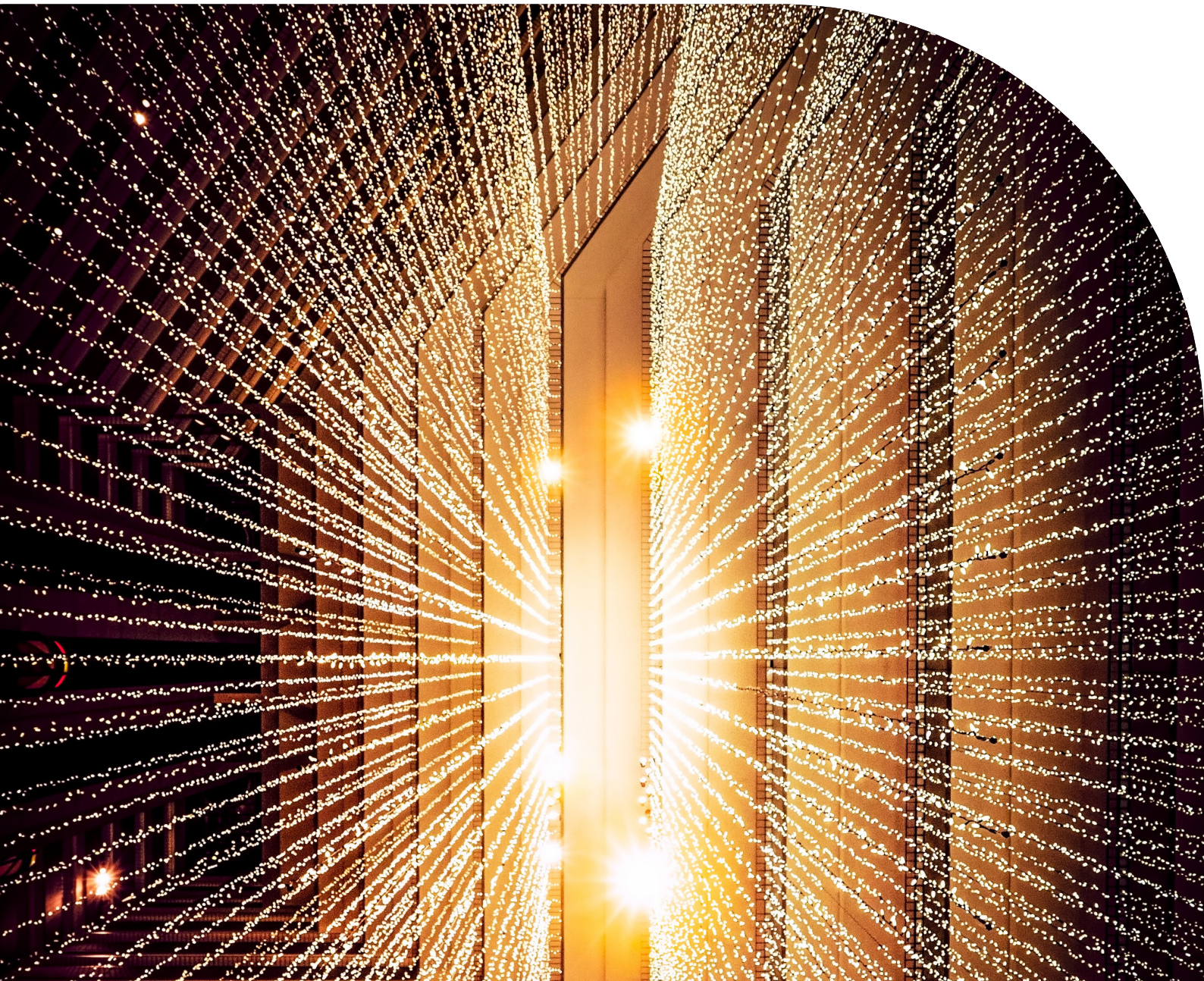
Grant Thornton

Unveiling the financial crime/ Anti-Money Laundering (AML) dynamics of Ireland's payments sector

Written by Jennifer Flannery

May 2024



Introduction

Over the last decade, we have watched technology revolutionise traditional financial practices, from the introduction of mobile banking apps to today's widespread use of electronic money and virtual assets. In the dynamic landscape of financial technology, Ireland stands out as a host of Payment Services Providers (PSPs) including both Payment Institutions (PIs) and E-Money Instiutions (EMIs), both indigenous and drawn by its buoyant fintech sector.

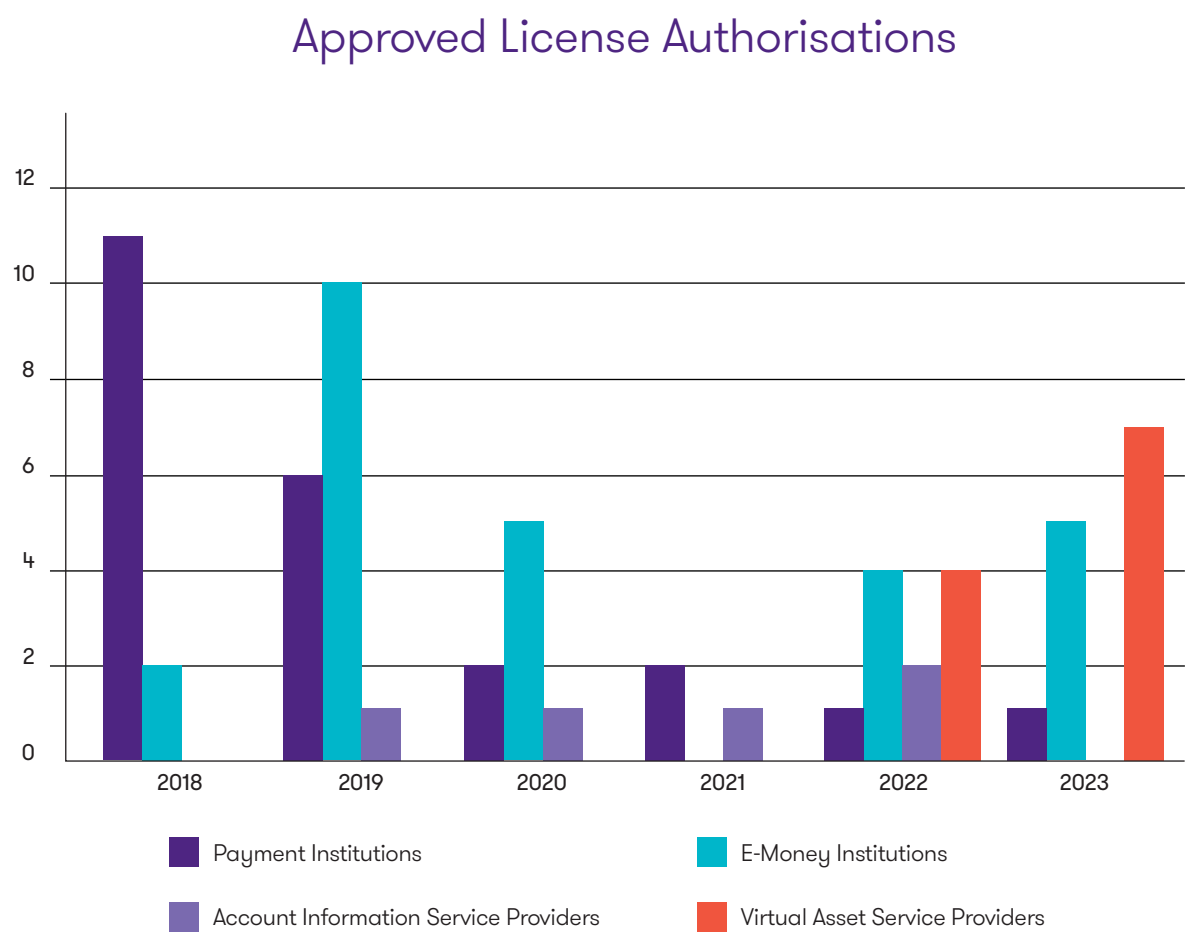
PIs emerged in 2018 with a record number of authorisations by the Central Bank of Ireland. Following this, there was a surge in EMI authorisations in 2019. This can be attributed to the wide range of strategic advantages offered by Ireland in addition to the robust regulatory framework applicable to PIs and EMIs that are overseen by the Central Bank of Ireland.

Ireland has been an important beneficiary of the UK's withdrawal from the European Union (EU) as companies are looking to shift operations and use Ireland as a launchpad to passport elsewhere in the EU, through either branch operations or cross-border services. The country's appealing tax policies, and a comprehensive network of double tax agreements, enhance its attractiveness as a jurisdiction for PIs and EMIs.

Furthermore, Ireland's regulatory environment around PIs and EMIs, as highlighted in the recent Central Bank of Ireland's Regulatory & Supervisory Outlook report (the Report)[1], is closely aligned with key European guidelines and, in particular of, EBA Guidelines on Outsourcing Arrangements. This alignment underscores Ireland's commitment to internationally recognised standards and emphasises the role financial crime plays in safeguarding the integrity of the financial systems. The Report outlines other crucial priorities for ensuring effective safeguards and robust governance structures, as well as enhancing risk management practices and strengthening efforts in Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) measures.

1. Central Bank of Ireland, Regulatory & Supervisory Outlook, Feb 2024

Introduction



As of May 2024, there are 28 EMIs, 25 PIs, six Account Information Service Providers (AISP) and 11 Virtual Asset Service Providers (VASP) authorised by the Central Bank of Ireland[2] marking a significant increase from 14 to 70 firms over the past seven years, although these figures may include multiple authorisations for certain PSPs. Based on figures from the European Central Bank (ECB) payment transactions, the value of sent payments involving non-monetary financial institutions for 2022 was €83,768.4 millions,[3] which is nearly a 300% increase on the figures from 2021.

Additionally, the Central Bank reported that, in Ireland there has been a 10-fold increase in safeguarded funds which was reported to be approximately €8bn in December 2023.[4] As this sector expands, a robust AML/CFT framework becomes even more crucial given money laundering schemes are becoming more complex and the growing prevalence in the financial system of other financial crimes, such as online fraud.

2. Central Bank of Ireland, 2024
3. European Central Bank, 2023
4. Central Bank of Ireland, 2024

Common AML Risks

1

Technology

Poor Data Quality
Inefficient ID&V

2

Outsourcing

Third Party Risk

Inadequate Due Diligence

3

Governance

Lack of Oversight

Gaps in System Controls

Technology

Many firms recognise that their current technology stack could benefit from smarter AML/CFT systems to sharpen financial crime risk detection and drive better governance and outcomes. As a result, there is a strong continuing trend towards upgrading legacy systems to balance changes in the financial system and customer expectations through the development of agile AML/CFT tech solutions which improve AML/CFT operational efficiency and effectiveness.

Some of the most common challenges include the integration of AML/CFT technology with existing systems, ensuring data quality, and the overarching cost associated with the implementation and maintenance of technology solutions. Firms which are part of a wider group often struggle to adapt to the technology platform provided by the group which make it challenging to build operational efficiencies given it's not fit for purpose, and maintain operational continuity.

One example of this includes the inability to integrate data from multiple sources making it difficult to establish a holistic view of customer transactions and behaviours. This disjointed approach can impede accurate risk identification, monitoring and red flag detection.

From our experience in working with PSPs and EMI firms, a comprehensive analysis has revealed a myriad of risks within the landscape of Identification and Verification (ID&V) processes. Key risks identified encompass the ability of users to maintain multiple accounts without system detection of duplicates, raising concerns on complete CDD and unified customer files.

Furthermore, the process of discounting/escalating evidence of tampering during the ID&V process was marked by uncertainty, with no documented procedure for addressing doubts about document authenticity.

Common AML Risks

Outsourcing

Outsourcing without appropriate safeguards and oversight in place can adversely affect the robustness of PSPs control and risk management framework. Additionally, we are seeing an overlap between the new standards proposed with evolving regulations and new standards being proposed by the European Commission under the Digital Operational Resilience Act (DORA). Although outsourcing AML/CFT activities might offer cost effective solutions and greater operational efficiency, it is important to acknowledge that the use of third-party vendors and reliance on intra-group outsourcing also introduces its own set of inherent risks, such as:

- The quality in KYC documentation is less than expected and does not meet the standards of the hiring firm or regulator.
- Inadequate data privacy/security measures with regard to processing and accessing sensitive customer data.
- Outsourced AML/CFT operational functions, resulting in less control and/or understanding over processes and procedures.

Overall, the biggest risk faced by firms in utilising third party services is regulatory non-compliance, which can result in financial repercussions and severe reputational damage. As a designated person, subject to the Criminal Justice Act[5], it is imperative to remember that although firms can outsource the activity, firms cannot outsource the risk.

Governance

The Central Bank of Ireland places a strong emphasis on establishing robust governance and controls, insisting that companies conduct thorough risk assessments for money laundering (ML), terrorist financing (TF), and financial sanctions (FS) risks. This evaluation should encompass a wide spectrum, including products and services/transactions, customer demographics, geographical operations, and distribution channels.

In building a solid AML/CFT governance framework, it is crucial to develop policies and procedures that align with both Irish AML/CFT legislation and EU FS regulations. These should cover critical areas such as customer due diligence (CDD), suspicious transaction reporting (STR), transaction monitoring, financial sanctions, record-keeping, training, and assurance testing. Adherence to customer due diligence (CDD) requirements is paramount, ensuring the ability to identify a firm's customer base and report on suspicious transactions and activities.

Recent interactions with payment and e-money firms have brought to light a multitude of noteworthy risks and challenges in financial crime governance and controls framework, such as:

- Incomplete integration of risk ownership within the first line of defence, resulting in deviation from established guidance by Central Bank of Ireland.
- Lack of feedback loops associated with the issue management process to ensure the efficient escalation, tracking, and appropriate senior management oversight on identified gaps in the financial crime control framework.
- Deficient approval channels and regular review cadence across policy and procedure documentation.

The overarching concerns identified above represent a pivotal vulnerability in AML/CFT governance and controls which calls for implementation of suitable oversight and governance mechanisms to facilitate the execution of corrective measures aimed at strengthening the controls within the AML/CFT system.

5. Criminal Justice Act 2010

Sustainable AML Practices

A proactive approach to mitigating the threat of the financial system being used to facilitate illegal activities and bad actors is essential. This can be achieved through the adoption of an AML strategy that is both sustainable and resilient in nature in line with the Central Bank of Ireland's current strategic commitment to *"strengthening our ability to maintain the resilience of the financial system"*.[6]

Technology

In the dynamic landscape of payment and e-money firms, technology stands as the linchpin driving efficiency, compliance, and innovation. As these financial entities navigate intricate processes like customer due diligence (CDD), the integration of cutting-edge technology becomes not just advantageous but indispensable.

Regulatory technology (RegTech), emerges as a transformative force empowering organisations to navigate complex regulatory frameworks efficiently and effectively. RegTech encompasses a suite of technological solutions tailored to streamline compliance processes, enhance risk management, and fortify adherence to regulatory standards. As industries grapple with an increasingly intricate web of rules and requirements, RegTech becomes a strategic ally, leveraging innovations such as artificial intelligence, machine learning, and data analytics to automate and optimise compliance workflows.

Manual CDD processes can be a time-consuming and onerous task. Arduous CDD administration has been eased in the last few years, owing mainly to the technological strides made within the industry. Leveraging digital know-your-customer (KYC) technology, particularly ID&V, streamlines the onboarding and periodic refresh process, enhancing accuracy and ensuring compliance with the most up-to-date regulations and expectations.

These RegTech platforms have a wide range of capabilities, from utilising biometric data e.g. live detection and facial matching, to performing authenticity and veracity tests on documents through numerous data checks. Not only is RegTech cost effective and time efficient, it also reduces the likelihood of human error.

In saying this, Firms need to be cognisant of a number of factors when evaluating these systems, such as:

- Oversight and quality assurances (QA) of group technology.
- Compatibility with legacy systems.
- Strong ID&V mechanism covering all aspects of policies and procedures.
- Scalability with the business as it grows.
- Ability to perform and function as expected under pressure e.g. increased traffic.
- Customisable features so that it can be amended to meet business requirements as highlighted within the business risk assessment and business strategy.
- Data management.
- Risk management practices e.g. cyber security: incident response, penetration testing; business continuity plans; disaster recovery.

6. Central Bank of Ireland, 2021

Sustainable AML Practices

Outsourcing

Outsourcing is a common facet of business models for both neo and traditional financial firms. It is imperative that when choosing an outsourced vendor which can extend beyond the average third party providers (i.e. fourth party and chain suppliers) to undertake elements of a firm's AML/CFT programme, the appropriate due diligence measures are employed. Overreliance on group/third party providers with weak controls and oversight arrangements continues to be a key risk in this sector.

There are many elements to consider before a firm can comfortably place reliance on a vendor. It is equally important to maintain oversight during the relationship. Relating to the outsourcing risks outlined above, we recommend:

- Confirming that the vendor conducts thorough due diligence on third party providers (i.e., forth parties of the authorised firm) by using standardised procedures across all relevant appropriate risk domains (e.g., financial stability, information security, data protection, risk management);
- Verifying that the vendor adheres to all standards, as set by relevant competent authorities, including data protection and AML /CFT regulations;
- Maintaining a collaborative relationship with the third-party vendor in order to keep informed on AML/CFT matters and involved in important decision-making processes.

Appropriate oversight and stringent alignment with regulatory requirements throughout the lifecycle of the outsourced relationship form the solid foundations of robust outsourcing frameworks.

Governance

In navigating the complex landscape of AML/CFT governance for payment firms, a comprehensive approach is imperative to address identified challenges and fortify controls. This dynamic environment necessitates tailored action points, aligning with the identified challenges, to foster a resilient governance framework.

From continuous system reviews to top-level leadership engagement and anticipatory measures, the following recommendations aim to fortify AML/CFT controls and ensure sustained effectiveness in the face of evolving financial crime risks. A strategic emphasis lies in tailoring controls to the unique risk landscape, ensuring a meticulous alignment with the individual firm's risk ecosystem.

- Ensuring that financial crime risks are clearly assigned to the appropriate line of defence (ie. 1LoD, 2LoD, and 3LoD). Regularly reviewing and updating risk owners to ensure appropriateness.
- Establishing a robust process for managing, escalating, and resolving issues identified through assurance testing. This process should include clear criteria for rating issues, oversight mechanisms, and tracking of remediation progress.
- Defining the scope of AML/CFT policies and procedures clearly to cover all organisational activities and including comprehensive descriptions of processes pertinent to internal business operations, such as transaction monitoring, customer due diligence, etc.
- Involving relevant stakeholders from the first line and second line, or the Board, in the review, finalisation, and approval of AML/CFT procedure documents. This ensures alignment with organisational objectives and regulatory requirements.

How can we help?

At Grant Thornton, we can help you stay ahead of the ever-changing regulatory environment across a number of AML/CFT areas, including but not limited to:

AML/CFT Framework reviews, AML/CFT assurance testing, Screening, Transaction Monitoring & KYC Managed Services

Frankie Cronin
Partner
Business Risk Services
T: +353 1 646 9044
E: Frankie.Cronin@ie.gt.com

Jennifer Flannery
Director
Business Risk Services
T: +353 1 500 8186
E: Jennifer.Flannery@ie.gt.com

David Henderson
Director
Business Risk Services
T: +353 1 500 8025
E: David.Henderson@ie.gt.com

Shane Quinn
Director
Business Risk Services
T: +353 1 433 2429
E: Shane.Quinn@ie.gt.com

How can we help?

CBI Mandated Risk & Control Assurance reviews & Safeguarding

Marie Mannion
Partner
Business Risk Services
T: +353 1 646 9044
E: Frankie.Cronin@ie.gt.com

DORA

Mary Loughney
Director
Consulting
T: +353 1 680 5728
E: Mary.Loughney@ie.gt.com

License Application Support

Dwyane Price
Partner
Prudential Risk
T: +353 1 436 6494
E: Dwayne.Price@ie.gt.com

Audit and Assurance

Maria Afontsenko
Partner
Banking and Insurance
T: +353 1 433 2570
E: Maria.Afontsenko@ie.gt.com

How can we help?

Tax Advisory & Reporting

Brian Murphy
Partner
Tax Financial Services
T: +353 1 680 5703
E: Brian.Murphy@ie.gt.com

Global Outsourcing

Gerard Walsh
Partner
Financial Accounting Advisory Services
T: +353 21 427 7513
E: Gerard.Walsh@ie.gt.com

Grant Thornton

grantthornton.ie