Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem

Newsletter

Financial Crime Bulletin

July 2026

Welcome to Issue 2 of the Central Bank's Financial Crime Bulletin, the first of two editions in 2026.

The purpose of the Bulletin is to provide an update on key regulatory developments in the areas of Anti-Money Laundering (AML), Combatting the Financing of Terrorism (CFT), Financial Sanctions (FS), Fraud and Market Abuse.

Financial integrity is about the financial system operating in a clean, transparent and accountable way. It is one of the Bank's four safeguarding outcomes and is directly relevant to our other outcomes – protection of consumer and investor interests, safety and soundness of firms, and financial stability.

We hope you find the information useful and if you have any feedback, you can contact us at FID_Administration@centralbank.ie

Inside this issue

Risks and Priorities

Financial crime continues to be an area of focus in policy, regulatory and law enforcement spheres in Ireland and Europe.

At national level, financial crime risks and priorities have been identified in the National Risk Assessment (NRA) published in June 2026. In regulation, the Bank has identified specific financial crime risks and vulnerabilities in the financial sector and has set out its priorities in the Regulatory & Supervisory Outlook Report 2026.

The NRA is the country's third comprehensive analysis of money laundering (ML) and terrorist financing (TF) risks, and its first formal assessment of proliferation financing (PF) risk. Together with the NRA, a new **Priority Action Plan** has been published with the aim of strengthening the State’s response to financial crime.

Risk Findings

In the NRA, overall ML threat for Ireland is rated as **Moderate**, with the highest risks generated by drug offences and fraud. Criminal networks are increasingly combining traditional cash-based methods with digital innovations, including use of crypto-assets and money mule networks. TF and PF threats are assessed as **Low**.

The NRA assesses fraud as a significant predicate offence for ML, with payment fraud reported by Irish payment service providers rising from €102 million in 2022 to €160 million in 2024, whilst fraudulent transactions more than doubled to 815,000. Investment fraud has surged dramatically, with reported losses exceeding €25 million in 2023, representing a four-fold increase in incidents since 2019. Notably, 44% of investment fraud reports reference cryptocurrency, reflecting criminals’ preference for rapid fund movement beyond regulatory reach.

Within the financial sector, traditional retail banks, digital banks, e-money institutions, and payment institutions are rated as **Very Significant** for ML and TF risks due to their scale, international exposure and the nature of products available.

Similarly, crypto-asset service providers (CASPs) present heightened ML and TF risks and are assessed as **Very Significant**. The sector's rapid evolution, including decentralised finance platforms and privacy-enhancing technologies, complicates detection efforts.

The NRA is an important source for regulators and regulated firms to inform their own ML/TF risk understanding and to identify areas of focus for risk mitigation. It will support firms in enhancing their risk-based approach and the Central Bank would encourage all regulated entities and designated persons to read it.

Regulatory & Supervisory Priorities

The Central Bank inputted into the NRA and is incorporating the findings into its regulatory and supervisory approach.

In addition to the NRA, the Central Bank assesses financial crime risk in the sectors it regulates and sets specific supervisory priorities. These priorities are outlined in the Central Bank’s Regulatory & Supervisory Outlook (RSO) Report, which is a useful source of information for compliance professionals.

In summary, the RSO identifies the banking, payments and e-money sectors as key priority areas for supervision, given they are inherently high risk from a money laundering/terrorist financing (ML/TF) perspective. We will also continue to closely supervise the investment fund sector given the nature and size of this industry in Ireland

Banking

In the banking sector, AML/CFT frameworks are generally mature and well embedded due to the efforts made over the past decade. However, a few areas have been highlighted in the Report:

- As the banking sector diversifies in Ireland, there is a need for newer entrants to continue to build and strengthen their AML/CFT frameworks, in line with national and European requirements.
- Boards and senior management must be able to demonstrate an understanding of their firm's key ML and TF risks and the adequacy of their risk management and control frameworks.
- There is a need to be particularly vigilant and responsive to criminals exploiting new technologies and practices to abuse the system, and firms within it.
- In respect of preventing and detecting fraud, banks must do more to strengthen their controls, including improving data and management information, and enhancing transaction monitoring and IT security systems to reduce the likelihood of frauds and scams occurring.
- Where fraud does occur, banks need to provide appropriate and timely support to affected customers.

Payment and E-Money

The payment and e-money sectors have inherently high exposure to the risk of financial crime, including money laundering, terrorist financing and fraud. This is because the business models in this sector are diverse and complex, typically handling a high volume of transactions with a wide international reach.

The use of technology and innovative ways to serve the needs of consumers is welcome for reasons of both efficiency and convenience. However, they expose vulnerabilities that can be exploited by criminals.

While some firms have taken positive steps to strengthen their AML/CFT risk management and control frameworks, much deeper work is required across the sector in this area. Firms' governance arrangements, systems and controls, including reporting mechanisms, need to be effective and proportionate to the nature, scale and complexity of their business, and the risks to which they are exposed.

There has been an expansion of cybercrime and fraud in recent years, with AI-driven social engineering becoming a primary threat, and this continues to challenge the sector's defensive capabilities.

Investment Funds

Financial crime continues to require attention in this sector. Funds can be exploited for money laundering and terrorist financing, with the funds sector in Ireland being the subject of international scrutiny from an AML/CFT perspective given its size and reach. It is a key area of focus for the Central Bank and we are currently undertaking a thematic review of suspicious transaction report (STR) reporting in the sector.

Crypto Assets

The opaque and rapidly evolving nature of the market structures in the crypto-asset sector can make detection and tracing of ML/TF activities particularly challenging.

Due to limited sector experience of evolving typologies, fast onboarding, complex cross border flows and fragmented know-your-customer and transaction monitoring, AML/CFT remains a key supervisory focus.

We expect firms to maintain effective AML and fraud-prevention controls to mitigate financial crime risks, and this will continue to be a key element of our supervisory focus this year and beyond.

Supervisory Expectations

The Central Bank has also outlined its priorities and expectations of firms through public engagements. This has included remarks delivered in April by the Director of Horizontal Supervision, Patricia Dunne.

Our key messages to firms on managing financial crime risks are:

- Understand your risks specific to your business;
- Invest in and enhance controls, recognising systems and models rely on good quality data and appropriate calibration;
- Where systems failures occur, prompt handling and reporting of the issue within the firm (and to the regulator) minimises both harm and regulatory risk;
- Report suspicious activity promptly and effectively; and
- Embrace technology with care, managing the risks to consumers and investors and to the firm itself.

Data Collection Update

Our enhanced Risk Evaluation Questionnaire (REQ) is a critical data collection tool to identify firm-level, sectoral and cross-sectoral risks and to inform our supervisory approach. They capture detailed quantitative and qualitative information on ML/TF risks and on the quality of firms' controls.

Roll out of Sector Specific REQs

In our December Bulletin, we gave an update on the rollout of our sector-specific AML/CFT Risk Evaluation Questionnaires (REQs). These new REQs serve three key purposes: meeting our European AML/CFT requirements, informing our supervisory strategy and decision-making, and identifying emerging and thematic trends.

Sectors covered to date

We have already published sector-specific REQs and guidance for the following sectors:

- Credit institutions;
- Payment institutions and electronic money institutions;
- Investment firms;
- Crypto-asset service providers;
- Life insurance companies; and
- Credit unions.

We will continue rolling out enhanced REQs for other regulated sectors in H2 2026. Each sector-specific REQ will be published on our website, and we will contact firms individually about their submission obligations.

REQ submission dates going forward

In 2026, we are staggering submission dates for sectors submitting REQs relating to 2024 and 2025 data. This phased approach allows firms time to familiarise themselves with the new REQs and data requirements, enabling them to implement changes effectively.

From 2027 onwards, we aim to standardise submission dates for **all sectors** as follows:

- **March 2027**: REQs relating to 2026 data. This is to align with AMLA's reporting framework.
- **From 2028 onwards**: Annual submission in March, based on the preceding calendar year's data.

We are grateful for industry engagement and feedback to date on the sector-specific REQ programme. We look forward to continuing that engagement.

AMLA Developments

In the previous edition of this Bulletin, we provided an overview of the new AML framework that will be introduced by the EU AML Package and an overview of AMLA's work programme for 2025[1].

In February 2026, AMLA published its Single Programming Document (SPD) for 2026 to 2028. The SPD gives an insight into AMLA's approach to prioritising certain technical standards and guidelines, aligning with its strategic objectives across three core deliverables:

- Completing the Single Rulebook;
- Advancing supervisory convergence; and
- Strengthening cooperation among Financial Intelligence Units (FIUs).

Annex XI to the SPD provides an overview of AMLA's scheduled mandates for 2026.

The main structures of AMLA are now well established in the shape of the Executive Board and the General Board.

AMLA is run by an Executive Board and an Executive Director (responsible for the day-to-day operations of AMLA).

The General Board is comprised of the Executive Board and national representatives. It meets in two alternative compositions:

- A supervisory composition with the heads of supervisory authorities responsible for AML/CFT supervision from all EU Member States (including the Central Bank); and
- An FIU composition with the heads of the FIUs from all EU Member States (including Ireland's FIU).

To support the work of the General Board in supervisory composition, it has established two Internal Committees:

- Internal Committee on the Functioning of the Supervisory System
- Internal Committee on Private Sector Standards

These committees consider and approve the work on the numerous technical standards and guidelines that needs to be prepared under the new EU AML framework. The work on the standards and guidelines is being done by working groups and taskforces comprised of staff from AMLA and national supervisory authorities.

The Central Bank is represented on both Internal Committees as well as key working groups and taskforces.

It is critical that firms remain alert to – and engage with – AMLA's public consultations on draft regulatory technical standards, implementing standards and guidelines.

[1] See Issue 1 of the Financial Integrity Bulletin here

AMLA is encouraging firms to participate in its ongoing public consultations and public hearings, so that firms can play their part in shaping the Single Rulebook and ensuring that the AML framework that emerges will be credible, resilient and operationally effective.

On 9 June, AMLA held its first conference under the theme: "Building Trust, Enhancing Integrity: A New Chapter in the EU's Fight Against Financial Crime.

The Central Bank also welcomes feedback from the private sector on the changes being made at EU level and we have been engaging with industry representative bodies and firms. This feedback is invaluable in shaping our views and interventions at AML board, committees and working group levels.

Tackling Fraud and Scams

There is a significant increase in the frequency and complexity of financial scams and frauds targeting consumers due to the rapid development and adoption of digital financial products, services and distribution channels[2].

In June, the OECD published *Protecting Consumers from Financial Frauds and Scams*, a report exploring how policymakers and public authorities can better protect consumers from them.

The report examines the drivers of the increased incidence of financial scams and frauds, articulates a typology of financial scams and frauds targeting financial consumers, and identifies effective financial consumer protection and financial education approaches to protect consumers from financial scams and frauds. It draws on data collected from 69 jurisdictions (of which 26 are OECD Members), representing the perspectives of 102 public authorities.

Speaking on the OECD report, Central Bank Deputy Governor for Consumer and Investor Protection, Colm Kincaid, said comprehensive action is needed by all actors in the system. This includes the Central Bank ensuring that the key insights from the report inform our regulatory and supervisory responses. Similarly, regulated financial institutions must continue to enhance their safeguards against fraud and put better supports in place for consumers who fall victim to fraud. And continued work is required to directly empower consumers by providing them with the tools, skills and competencies they need.

Separately, research published by the Central Bank in April reveals that more than one in three Irish adults have experienced frauds and scams, with nearly two-thirds of victims suffering financial losses. Concerningly, a striking 38% of fraud victims never reported their experience to their financial service provider or any authority. The study reveals a clear correlation between reporting fraud and recovering lost funds. Among victims who reported fraud to their bank, An Garda Síochána or another relevant authority, 57% were able to recover money. By contrast, only 13% of those who didn't report the fraud recovered money.

No single agency or firm can effectively combat digital financial fraud. Success requires coordinated effort across the financial and non-financial sectors and sustained inter-agency collaboration.

At the Central Bank, our multi-pronged approach to this issue involves supervision of financial firms' efforts to prevent, detect and report fraud, and education, disruption and enforcement around fraud and unauthorised activities. We work closely with law enforcement authorities and other State agencies to tackle fraud.

We are currently carrying out a thematic review of authorised push payment fraud in the banking and payment sectors, on foot of which we expect to issue updated supervisory expectations for firms. We expect firms to

[2] As noted in the OECD Report here

have measures in place to prevent, detect and report fraud and take a consumer-centric approach to support their customers when they fall victim to frauds and scams.

In our work on unauthorised activity, we are noting an increase in reports about fraud loss recovery scams to the Central Bank. These schemes involve scam artists contacting victims of fraud and claiming they can help recover lost funds for an upfront fee. These fraudsters often using fake documents or impersonate officials, and their real objective is to steal more of the victims' money. This scam is designed to exploit victims' desperation, often leading to more financial loss.

The Central Bank recently participated in the Global Finfluencer Week of Action. Actions taken by us included the publication of two separate strands of content: one aimed at promoting responsible finfluencing, and the second at educating consumers on how to protect themselves. We held a discussion forum with a large group of young adults to understand their experiences of finfluencing and to gain insights. Together with colleagues from the Advertising Standards Authority and the Competition and Consumer Protection Commission, we held a roundtable with five prominent finfluencers, which was educational and informative for all participants.

We also seek to disrupt frauds and scams by breaking the link between the perpetrators of the frauds and scams and the victims. In April, we published our first Report on our Activities under the Digital Services Act.

EU Financial Sanctions and Trusts

There have been three landmark judgments delivered by the European Court of Justice clarifying how EU asset-freeze sanctions apply to assets held in trust structures[3].

Key Finding

The Court established that EU sanctions extend to trust assets if a sanctioned individual exercises **substantive control or influence** over them, rather than merely holding formal legal title. This means that formal trust structures alone cannot shield assets from sanctions.

The judgments establish a "substance over form" test. This mean that economic operators must look beyond legal documentation and conduct thorough, case-by-case evaluations of whether a sanctioned

What this means

The judgments establish a "substance over form" test. This mean that economic operators must look beyond legal documentation and conduct thorough, case-by-case evaluations of whether a sanctioned person retains control/influence over the trust assets. When conducting an evaluation, economic operators should consider:

- Conducting reality-based control analysis rather than relying on formal legal structures;
- Conducting a granular review of trust deeds including but not limited to the rights, amendment powers, and governance patterns contained in the trust deeds; and

[3] *Delivered on 21 May 2026 – see Case C-483/23 (T Trust), C-428/24 (FZ AR) and C-476/24 (SX)*

- Assessing evidence of actual influence and benefit, including patterns of de facto or informal arrangements which provides a listed person with the ability to benefit from the trust assets in any way.

The purpose of conducting this analysis is to assist economic operators in satisfying themselves that they are not engaging in unlawful activity.

If due diligence uncovers a reasonable ground for suspicion that a sanctioned individual exercises substantive control or influence over a trust structure or if there are suspicions of sanctions circumvention, then trust assets should be frozen and immediately report the activity to Garda Siochana and the Financial Sanctions Team in the Central Bank of Ireland at sanctions@centralbank.ie

Reporting Market Misconduct

Market abuse is a category of financial crime that undermines the integrity, transparency, and fairness of financial markets - its prevention is one of the Central Bank's core aims as Ireland's markets regulator.

Market abuse is very difficult to identify so Suspicious Transaction and Order Reports (STORs) are critical in providing valuable intelligence that can assist the Central Bank in detecting and investigating market misconduct that might otherwise remain hidden.

In recent years, the Central Bank has consistently emphasised the importance of STOR reporting and that firms are often best placed to identify unusual trading patterns or behaviours. This is borne out by the fact that the majority of our live enforcement investigations began life with a STOR.

Our expectations are therefore unchanged that firms need to be proactive in STOR reporting and we want to see their reporting backed by effective surveillance, robust escalation procedures and timely reporting.

Although the volume of STOR reporting, like the size of our markets, has increased in recent years we believe certain firms/sectors can do more and we are currently conducting a thematic assessment of market abuse frameworks in a cross-section of firms. The findings will provide us with insight on where firms, and indeed the Central Bank, can do more.