Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem

Issue 1

December 2025

Financial Crime Bulletin

Welcome to this first edition of the Central Bank's Financial Crime Bulletin (following on from the previous AML Bulletin series).

The purpose of this biannual 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), and Fraud.

This has been a year of change in the AML regulatory and supervisory framework. At national level, we in the Central Bank have moved to an integrated supervisory approach where we consider risks and supervisory activities more holistically. This is true too for financial crime risks where we consider AML/CFT, Financial Sanctions and Fraud across the financial system and how best to address them. At European level, AMLA is now operational, work is continuing to implement the EU AML Package, and MiCAR entered full force.

In this Bulletin, we provide updates on the following:

- Risk Assessment
- Crypto & Payments
- Fraud and Scams
- Financial Sanctions
- EU AML Developments

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

"Safeguarding the integrity of the financial system and consumer interests by combatting financial crime needs to be a priority for all firms and agencies involved with financial services"

Deputy Governor Colm Kincaid

Risk Assessment

The focus on identifying and assessing ML/TF/PF risks at all levels is an ongoing process.

National Risk Assessment

At the national level, Ireland's National Risk Assessment (ML/TF/PF) is currently being updated. An NRA aims to provide both the public and private sectors with an understanding of the main ML/TF/PF threats and vulnerabilities in a country. We have been inputting into this process in respect of our regulatory mandate and supervisory population.

Sectoral and Firm Specific Risk Assessment

The Central Bank identifies and assesses ML/TF/PF risks across all sectors and firms within its AML/CFT regulatory population. We consider inherent risks (threats/vulnerabilities) and mitigation measures (controls) to arrive at a residual risk score for each sector and each individual firm. This rating then drives the level and extent of supervisory activity on a given sector /firm (along with trigger events and intelligence).

Data collection

To identify and assess risks, we rely on a variety of data sources, including an AML/CFT Risk Evaluation Questionnaire (REQ). We are introducing an enhanced REQ that allows us to be more data driven and will enables us to meet new European AML/CFT requirements.

Over a phased timeframe, we are replacing the current generic REQ with sector-specific REQs to capture more detailed and insightful risk data. We will use the new sector specific REQs to inform our decision-making and supervisory strategy both at firm and sector level and to assist in identifying emerging and thematic trends.

In June 2025, we published the first two sector specific REQ templates and guidance on our website for (1) Credit institutions; and (2) Payment institutions/Electronic money institutions.

We will continue to roll out the enhanced REQs for other regulated sectors between now and early-2027. As part of the roll out, each sector-specific REQ will be published on our website. We will contact firms individually in regard to their submission obligations and we welcome all engagement on this issue.

Monitoring and review of risk assessments

Risk assessment and customer due diligence are two essential elements of any effective AML/CFT framework. This includes all customers regardless of size and scale, including those who are not themselves designated persons for AML/CFT purposes.

Certain persons will not be treated as a designated person for AML/CFT purposes solely as a result of operating as a credit or financial institution (section 25(4) Criminal Justice Act 2010). Instead, they can qualify for an

For further detail on our enhanced REQs, see:

https://www.centralbank.ie/regulation/anti-money-laundering-and-countering-the-financing-of-terrorism/sector-specific-ml-tf-risk-evaluation-questionnaire

exemption if they meet certain criteria. These include that the annual turnover of the person's business attributable to operating as a credit or financial institution is €70,000 or less; and that the annual turnover of the business attributable to operating as a credit or financial institution does not exceed five per cent of the business's total annual turnover.

While exempt themselves, such persons will have relationships with larger firms which are designated persons. These larger firms must carry out a business risk assessment that identifies and assesses the ML/TF risk involved in the conduct of their own business activities. Furthermore, a firm must apply its business risk assessment when determining the extent of customer due diligence (CDD) required for a particular customer or transaction.

Firms need to have an up-to-date understanding of a customer's business and professional activities. Significant changes to customer activity and behaviour should prompt further review of the customer's business and professional activities to ensure that the firm has a comprehensive understanding of that customer and any potential ML/TF risks that it may present. Where required, additional customer due diligence should be conducted.

Crypto & Payments

With the Virtual Asset Service Providers (VASP) regime ceasing at the end of this year, work continues on the licensing of firms under the Markets in Crypto-Assets Regulation (MiCAR). To date, 6 firms have been authorised as Crypto Asset Service Providers (CASPs) by the Central Bank, with more anticipated in the coming months.

Regulatory updates

There have been a number of regulatory developments in the AML regulatory area for CASPs and firms engaging with crypto assets.

Most significantly, the Recast Funds Transfer Regulation (FTR) (in force since December 2024) applies to the transfer of certain crypto assets. It aims to enhance the transparency of transfers of funds and crypto assets by enabling relevant authorities to trace such transfers, in order to prevent, detect or investigate ML and TF.

Under Travel Rule Guidelines, Payment Service Providers (PSPs) and CASPs should take steps to detect missing or incomplete information that accompanies a transfer of funds or crypto-assets, and have procedures in place to manage a transfer of funds or a transfer of crypto-assets lacking the required information. These "Travel Rule Guidelines" became applicable on 30 December 2024. Importantly too, the European Banking Authority (EBA) has updated its Guidelines on ML/TF Risk Factors,

PSPs and CASPs are reminded of their obligation to have procedures in place to identify those PSPs or CASPs who repeatedly fail to provide the information which must accompany transfer of funds and certain crypto-assets transfers and to report these to the Central Bank. Further information on this obligation and how to make a report can be found here:

https://www.centralbank.ie/regulation/anti-money-laundering-and-countering-the-financing-of-terrorism/fund-transfer-regulations-notification-requirement-for-payment-service-providers

specifically in order to highlight factors that may indicate a CASP's exposure to higher or lower ML/TF risk and explain how CASPs should adjust their customer due diligence in line with those risks. The EBA also provides guidance to other regulated firms on risks to consider when engaging in a business relationship with a CASP or otherwise exposed to crypto assets. The EBA's Risk Based Supervision Guidelines have also been updated to include CASPs within scope.

Supervisory updates

The new EU AML Authority, AMLA, has placed an early spotlight on the crypto sector, as set out in its Work Programme (link). This emphasises the need for firms engaging in crypto asset activities to have in place strong protections against money laundering and terrorist financing.

From a supervisory perspective, AMLA has made it clear to national competent authorities (NCAs) – including the Central Bank – the need to avoid the risk of diverging application of AML/CFT requirements and inconsistent controls. AMLA has emphasised the need for licensing and supervisory authorities to ensure that CASPs have effective AML/CFT systems in place from day one of their authorisation.

The requirements of the crypto sector to have robust AML/CFT controls was highlighted in a recent Central Bank enforcement settlement. In this case, a virtual asset service provider was fined €21,464,734 for breaching AML/CFT monitoring obligations between 2021 and 2025. The main issue was faults in the configuration of the provider's transaction monitoring system, which resulted in more than 30 million transactions not being properly monitored over a 12-month period.

See the latest enforcement settlement details here:

https://www.centralbank.ie/news/article/press-release-enforcement-action-against-coinbase-europe-limited-6-November-2025

Fraud & Scams

Fraud and scams continue to grow through digitalisation and ever-increasing online activity. This area is recognised as a major issue for consumers, businesses and society. It is a priority for the Central Bank that measures are taken to prevent fraud and scams occurring through the financial system.

In a recent speech, our Deputy Governor for Consumer and Investor Protection, Colm Kincaid, delivered a message that the Central Bank's work will include raising consumer and investors' awareness of how to protect themselves against frauds and scams; using our status as Trusted Flagger to ensure that online platforms prioritise reports made by the Central Bank to them about illegal content; and detecting and punishing unauthorised providers and market abuse. (A Trusted Flagger is an entity accredited by Coimisiún na Meán – see further detail below).

He went on to say that we will assess fraud detection and prevention controls within mobile apps and other payments services. We will also work with other law enforcement and government agencies to improve our national framework in the face of the rising threat financial crime poses to our society.

The Central Bank recognises this as an issue that can only be comprehensively addressed through a collaborative response across many agencies and parts of our business community. We are committed to playing our part by fulfilling our regulatory mandate, and as part of the wider national effort working with other State authorities, bodies and groups.

Access Deputy Governor Kincaid's speech here:

https://www.centralbank.ie/news/article/speech-by-deputy-governor-colm-kincaid-at-financial-services-ireland-02-0ctober-2025

Some of the measures we are taking to tackle fraud and scams include:

Spotting scam artists

We launched, in early November, a further public-facing campaign aimed at reinforcing our message to consumers around how they can safeguard their finances from fraud, while generating awareness about certain common scam types and techniques (such as fake comparison websites, deepfake scams and fraud loss recovery schemes). Further information about the campaign can be found at this link.

We have also included in this campaign messaging about staying safe online and we continue to emphasise the importance of the SAFE test:

We welcome industry's continuing efforts in this space to raise awareness with consumers and to help them avoid scams and frauds.

Disrupting scam artists – Trusted Flagger

The Trusted Flagger initiative was introduced under the Digital Services Act. In short, online platforms are required to prioritise reports about suspected illegal content made by Trusted Flaggers. Coimisiún na Meán, as Ireland's digital services co-ordinator, awarded 'Trusted Flagger'

status to us in April 2025, the first such appointment in Ireland. The Central Bank's stated area of expertise is financial scams and frauds, including the provision and/or offer of financial services without authorisation. Online platforms are now legally obliged to ensure that any illegal online content reported by us regarding financial scams and fraud is prioritised by those platforms and dealt with in a timely manner.

Central Bank awarded Trusted Flagger status. See:

https://www.cnam.ie/the-central-bank-of-ireland-awarded-trusted-flagger-status/

Financial Abuse

The Central Bank will assess and supervise fraud risk in the system and mitigation measures by firms. This will be underpinned by implementation of the revised Consumer Protection Code, which contains measures to prevent financial abuse under the Standards for Business Regulations, among other measures.

The financial abuse provisions are effective from March 2026. They require firms to control and manage their affairs and systems to counter the risks to customers of financial abuse. Firms are also required to communicate clearly to their customers the risk of financial abuse, including where the firm is aware of the occurrence of digital frauds or scams, the supports available and the actions customers can take where they are a victim of financial abuse.

Financial Sanctions

Since 2022, there has been significant work undertaken within the EU Financial Sanctions (Restrictive Measures) regime in response to Russia's invasion of Ukraine. This has led to some welcome changes to the EU and national regulatory framework to strengthen compliance with financial sanctions and introduce clear obligations around preventive measures that firms need to have in place.

Regulatory updates

The Funds Transfer Regulation was amended to oblige PSPs and CASPs to have preventative measures frameworks in place to comply with EU Restrictive Measures (effective since December 2024).

Subsequently, the EBA issued Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures that for the first time provide much needed clarity on firms' obligations across the Union.

- The first Guideline sets out provisions to ensure that financial institutions' governance and risk management systems are sound and sufficient to address the risk that they might breach or evade restrictive measures (financial sanctions)

- The second Guideline is addressed to PSPs and CASPs and specifies what they should do to be able to comply with restrictive measures when performing transfers of funds or crypto assets.

Both Guidelines have been adopted by the Central Bank and are effective from 30 December 2025 (in addition to the new requirements adopted under the FTR in December 2024). Firms will need to familiarise themselves with the new requirements and guidelines and take necessary action to ensure they are compliant.

A restrictive measures exposure assessment will help firms to evaluate where they are exposed to risks of non-compliance with restrictive measures and the risks of circumvention of restrictive measures, based on their activities and customer base. However, firms are reminded that such an assessment does not change that firms still have an obligation to comply with restrictive measures and that the measures to comply may be part of future Central Bank supervisory engagements.

Supervisory updates

In addition to the changes in the regulatory framework, work has continued on assessing the risks and supervising mitigation efforts in firms. We assessed the efficacy of financial sanctions screening systems of 40 firms across a wide range of sectors in a thematic review completed in 2024.

Our aim was to assess the effectiveness of customer and transaction screening systems (including configuration) utilised by firms. Some of the key findings included:

- **While all firms had client screening systems, just under half of those sampled did not have transaction screening systems, which potentially exposes them to a greater risk of breaching sanctions requirements.** In such cases, a firm needs to ensure that decision is subject to robust governance and clearly documented.

- **Many firms' screening systems were of a satisfactory standard in terms of identifying sanctioned names when undertaking customer and transaction screening.** However, there were some firms' screening systems that were well below a satisfactory standard. This highlights the importance of ongoing, regular and appropriate testing of systems to ensure they are operating effectively and to identify any areas for improvement. Additionally, where firms have outsourced their screening systems they must ensure that they have appropriate oversight of the outsourced service providers and the screening tool; and

https://www.centralbank.ie/regulation/how-we-regulate/international-financial-sanctions/financial-sanctions-updates

- **When the test data was manipulated to reflect common data quality issues, the effectiveness of customer and transaction screening systems decreased.** This highlights the need to test and assess the effectiveness of fuzzy logic rules on an ongoing basis. Where an issue (or a breach of EU sanctions) arises, immediate action should be taken to address it.

Since 2024, we have noted an increase in breach reports received in relation to sanctions circumvention. Firms should identify and assess which areas of their business are particularly vulnerable or exposed to restrictive measures and to potential circumvention of restrictive measures. On this basis, they should put in place, implement and maintain up-to-date policies, procedures and controls to ensure that they can comply effectively with restrictive measures regimes. Sanction compliance policies, procedures and controls should be effective and proportionate to the size, nature and complexity of the financial institution, and to its restrictive measures exposure. These policies should be kept under regular review by each firm.

International Card Schemes

A potential sanctions risk for Irish banks, PSPs, ATM operators and merchants services relates to the use of non-EU cards for transactions and withdrawals at EU ATMs.

ATM transactions are often facilitated through international card schemes which use Bank Identification Numbers (BINs) to identify the card-issuing bank. Due to the global nature of these schemes, cards issued by banks or entities subject to EU financial sanctions may still be used at EU ATMs unless those BINs are specifically blocked.

We are aware of specific instances of processing card transactions involving US cards issued by a Belarussian bank, Belgazprombank, which is under EU restrictive measures since 25 February 2025.

There is a risk that there may be other designated entities who are subject to EU restrictive measures which have issued products that need to be blocked by Irish banks, PSPs, ATM operators and merchant services. Failure to do so poses a heightened risk of breaching EU sanctions.

It is important to be aware that card schemes apply their own compliance controls and they may not always reflect the full scope of EU sanctions, e.g. US card schemes may only reflect OFAC Regulations and not always EU Regulations.

There may be significant risk in relying solely on third-party schemes or networks to manage sanctions risks. Please note that ultimate

*Access the EU Circumvention Guidelines **here***

*Access the EBA Guidelines on implementing Union and National restrictive measures **here***

responsibility for compliance with EU sanctions rests fully with EU institutions.

Institution-specific controls and due diligence are essential to ensure that no funds or financial services are provided, directly or indirectly, to designated persons or entities.

If you identify or suspect a breach, please report it to the Central Bank by email to sanctions@centralbank.ie

EU AML Developments

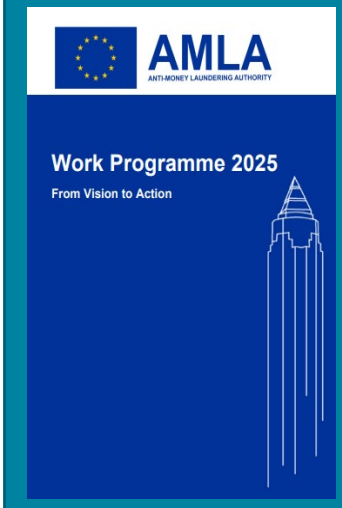
AMLA is now well up and running, with its chair, executive board and executive director in place, key staff being hired, and a number of working groups established to progress critical workplan items.

In its Work Programme (link), AMLA provides an overview of progress to date on key deliverables and objectives. AMLA will initially focus on working with NCAs and Financial Intelligence Units (FIUs) on drafting the regulatory technical standards, implementing standards and guidelines required under the AML Package.

These measures will help to ensure that both NCAs and obliged entities understand their obligations in advance of the AML Package implementation deadline of mid-2027. For the Central Bank and our regulated population alike, significant work is required now to make effective preparations. Firms should familiarise themselves with the AMLR, in order to ensure they are in a position to successfully implement the required changes once the AMLR becomes applicable.

In terms of delivering on the necessary regulatory technical standards, implementing standards and guidelines, AMLA has prioritised the following mandates:

- Regulatory technical standards on lower thresholds and criteria to identify business relationships (Article 19.9 AMLR)
- Regulatory technical standards concerning the AML/CFT central database (Article 11(6) AMLAR)
- Regulatory technical standards on home/host cooperation between NCAs (Article 46(4) 6AMLD)
- Implementing standards on cooperation within the AML/CFT supervisory system regarding direct supervision (Article 15(3) AMLAR)
- Guidelines on minimum requirements on business-wide risk assessment (Article 10(4) AMLR)



"2025 is the year AMLA takes shape — building trust, creating structures, and preparing to deliver on our mission to protect the Union against financial crime."

~ Bruna Szego, Chair of AML

AMLA has noted that the outcome of the dialogue between the European Parliament, the Council and the Commission on the simplification process could eventually lead to certain mandates being postponed.

As a member of AMLA's General Board, we welcome any insights and feedback into the development of the new regulatory framework and supervisory approach.