Q3 2024 - Financial Crime Quarterly Updates

July - September 2024

pwc

Introduction

Welcome to the latest edition of our Financial Crime update, which outlines all of the latest news and regulatory changes across the world of Financial Crime.

While it has been quieter over the Summer months, there was still key activity happening from a Financial Crime perspective, both locally in Ireland and further afield. Speaking at the Future of Financial Intelligence Sharing Event held in September, Deputy Governor of the Central Bank of Ireland, Derville Rowland, shared her remarks on 'The foundations for AML partnership in Ireland'. Ms Rowland focused on the establishment of partnerships for information sharing in Ireland connected to the new AML package. The Central Bank also officially opened applications for their new Innovation Sandbox Programme.

From a European perspective, the EBA published their work programme for 2025 and as always there is a focus on AML related activities. The key AML task for the EBA in 2025 will be a smooth transition to the new EU AML/CFT framework.

We hope you enjoy reading this newsletter, which contains further details on the issues outlined above, and more!

Sinead Ovenden
Partner, FS Risk and Regulation

Table of contents

Irish Financial Crime Updates

The foundations for AML partnership in Ireland - Remarks by Deputy Governor Derville Rowland

On September 25th 2024, at the Future of Financial Intelligence Sharing Event, Deputy Governor Derville Rowland shared her remarks on 'The foundations for AML partnership in Ireland'. In terms of partnerships for information sharing in Ireland, Ms Rowland highlighted three things that are required to make the new AML package a success:

1. AMLA and national supervisors need to encourage and support the establishment of Partnerships for the Sharing of Information.
2. The responsibility for making Partnerships for Information Sharing work under the AML Regulation does not rest on Authorities alone. Partnerships are not possible without the private sector playing its part.
3. AMLA and national authorities, including law enforcement, must work in collaboration to raise standards and act as a catalyst for innovative solutions, including around data sharing, to support the fight against money laundering and terrorist financing.

In relation to the Information Sharing provisions under Article 75 of the new AML Regulation, Ms Rowland confirmed that this provision will enable, for the first time, the sharing of certain confidential information between private sector operators under the auspices of what are known as "Partnerships for Information Sharing". With this provision there will be a balance between combatting ML/TF and the privacy and the data of all EU citizens. One guardrail that will be in place is the requirement that information can only be shared within a Partnership provided the information relates to customers deemed to be higher risk and the information sharing is strictly necessary for the purposes of meeting AML/CFT obligations.

The AML/CTF Supervisor role in these Partnerships will include encouraging the establishment of Partnerships through the development of clear guidance in addition to a verification process that is accessible, transparent, and capable of evolving over time. Ms Rowland noted that work is already well underway in the Central Bank for this. Supervisors will also have a role in fostering and supporting the development and adoption of technologies that facilitate the sharing of sensitive information through the use anonymisation technologies (Privacy Enhancing Technologies).

It was highlighted by Ms Rowland that responsibility for making Partnerships for Information Sharing work under the AML Regulation does not rest on Authorities alone. Partnerships are not possible without the private sector playing its part. It is for private sector operators to decide on when it is appropriate to establish a Partnership and who the participants of such a Partnership should be.

The full speech from Ms Rowland can be read here.

Applications for the CBI Innovation Sandbox Programme officially open

In September 2024, the Central Bank of Ireland (CBI) officially opened applications for their Innovation Sandbox Programme, with the theme of “Combatting Financial Crime”. With the opening of applications, further details were provided on the Framework of the Programme, which will include:

- A structured programme of workshops, each month on topics relevant to combatting financial crime;
- Ongoing bespoke engagement with dedicated Sandbox Relationship Managers, who will act as their point of contact to oversee and coordinate participation throughout the Programme; and
- Access to a Data Platform, for participants to test and develop their innovation.

In describing the challenge, the CBI notes that “Financial crime is not just an issue for the financial sector, but for other sectors too. One of the key factors in successfully reducing financial crime is for firms and wider partners to work collaboratively by sharing data and intelligence”.

A set of six problem statements have been outlined by the CBI, including:

- **Collaboration:** Can collaboration and information-sharing between and within the financial system, technology providers and other stakeholders enhance the effectiveness of anti-money laundering and counter terrorism financing efforts?
- **Consumer protection:** How can efforts to combat financial crime ensure that the solutions do not compromise privacy, data, security or consumer protection?
- **Regulatory adaptability:** What are the impacts of the changing trends and emerging technologies in financial crime on the regulatory frameworks? To what extent do the current regulatory frameworks enable or hinder the use of technology to combat financial crime?

Applications for the Innovation Sandbox Programme will be accepted until **23:00 on 31 October 2024**, with the programme commencing in December 2024. Further details can be found here.

Central Bank of Ireland: Transformation of Regulation and Supervision

In September 2024, the Central Bank of Ireland (CBI) announced plans for transforming its approach to regulation and supervision, aligned to its overall Strategic Plan. In delivering the relevant changes, the CBI is focusing on four key aspects:

- Accelerating the evolution of their risk-based supervisory approach such that it becomes more data-driven, agile and scalable;
- Harnessing innovation in how they work through developing their data and tools (including supervisory technology);
- Anticipating and supporting innovation in financial services; and
- Preparing for the new EU anti-money laundering requirements and the establishment of the new EU agency AMLA.

In relation to its supervisory approach, the CBI announced that their risk based supervisory model is evolving to deliver a more integrated approach to supervision, drawing on all elements of the mandate of the CBI (consumer and investor protection, safety and soundness, financial stability and integrity of the system). The new operating structure will include seven directorates, which will report into the existing Deputy Governors for Financial Regulation and Consumer and Investor Protection:

- There will be three directorates responsible for sectoral supervision; a Banking & Payments Directorate, an Insurance Directorate and a Capital Markets & Funds Directorate. All three directorates will have integrated teams responsible for all elements of the mandate of the CBI and supervising risks as they relate to the sector. This means supervising to protect consumer and investor interests, safety and soundness and the integrity of the system at a sectoral and an individual firm level.
- There will be a Horizontal Supervision Directorate working in partnership with the sectoral supervisory teams on a system-wide and thematic basis. It will provide specialist input on key cross-sectoral risks such as conduct, behaviour and culture, anti-money laundering and terrorist financing, financial resilience, operational resilience and technology risks.
- There will also be a Supervisory Risk, Analytics and Data Directorate, a Policy and International Directorate and an Enforcement Directorate.

The CBI plans to implement these changes in early 2025. The full announcement from the CBI can be viewed here.

FraudSMART Money Mule survey results launched

On September 18th 2024, FraudSMART, an initiative of the Banking & Payments Federation Ireland, published results from their 2024 Money Mules Survey. Some of the key findings from the Survey include:

- Over €44 million has been laundered through money mule accounts in last three years;
- One in three (34%) 18-24-year-olds admitted they would consider using their bank account to lodge or transfer money on behalf of someone else, in exchange for keeping some of the money;
- FraudSMART members identified almost 9,000 cases of money muling in last three years;
- Nearly half (45%) of 18-24-year-olds reported that they, or someone they know, have been approached to use their bank account to transfer money;
- 61% of parents of teenagers surveyed said they have not discussed the risks of money mules with their children.

In order to highlight the scale, dangers and consequences of money muling, FraudSMART launched a major awareness campaign through Snapchat and TikTok, with support from Minister Patrick O'Donovan and USI. As students return to college, the 'Don't be a mule' campaign is warning young people and parents to be vigilant, highlighting red flags to watch out for.

Further details on the survey results, as well as the FraudSMART campaign can be found here.

European Financial Crime updates

EBA Work Programme released for 2025

In September 2024, the EBA released its Work Programme for 2025, outlining how the authority intends to fulfil its mission and mandates for the year ahead. For 2025-2027, the EBA adopted five strategic priorities which broadly continue those of the previous programming document:

1. Finalise and implement an effective and proportionate Single Rulebook;
2. Foster financial stability in an economy transitioning towards sustainability;
3. Enable an integrated reporting system for enhanced assessment and disclosure;
4. Implement DORA oversight and MiCAR supervision; and
5. Focus on innovation for the benefit of consumers, and ensure a smooth transition to the new AML/CFT framework.

From an AML/CFT perspective, the main focus for 2025 will be the smooth transition to the new EU AML/CFT framework and AML Authority (AMLA). The main objectives of the EBA here will be:

1. To work closely with competent authorities and the European Commission to finalise the transition to the EU's new legal and institutional AML/CFT framework;
2. To put in place the structures necessary to make close and continuous cooperation between prudential and AML/CFT authorities possible in the fight against financial crime; and
3. To continue to lead the fight against ML/TF until the transition to the new legal and institutional AML/CFT framework is complete.

The EBA sees the main outputs from an AML/CFT perspective in their 2025 work programme to include:

Ongoing

- Tackling ML/TF risk through prudential supervision – embedding ML/TF aspects in the prudential framework (CRD/CRR, PSD/PSR, MiCAR);
- Monitoring ML/TF risks and trends (including through EuReCA);
- Supporting the transition to AMLA.

Quarter Two

- RTS on Central Contact Points;
- Opinion on ML/TF risks.

Quarter Four

- Response to the European Commission's Call for Advice on draft RTS and guidelines under the future AML/CFT framework;
- Final report on AML/CFT colleges;
- Final report on Assessments of competent authorities' approaches to the AML/CFT supervision of banks.

You can read the full Work Programme here.

EBA issues 'travel rule' guidance to tackle ML/TF in transfers of funds and crypto assets

On July 4th 2024, the European Banking Authority (EBA) published Guidelines on the so-called "travel rule", i.e. the information that should accompany transfers of funds and certain crypto assets. This rule will help tackle the abuse of such transfers for money laundering and terrorist financing purposes. These guidelines have been published following the introduction of Regulation (EU) 2023/1113, which extended Regulation (EU) 2015/847 (funds transferred by PSPs) to transfers of Crypto Assets.

The Guidelines provide detail on the steps for payment service providers (PSPs), intermediary PSPs (IPSPs), crypto-asset service providers (CASPs), and intermediary CASPs (ICASPs) to take to detect missing or incomplete information that accompanies a transfer of funds or crypto-assets, and the procedures they should put in place to manage a transfer of funds or a transfer of crypto-assets lacking the required information.

As with the original guidelines implemented for PSPs, these new guidelines place an emphasis on a risk-based approach, setting clear regulatory and supervisory expectations, while leaving sufficient room for allowing entities to define their approach in a way that is proportionate to the nature and size of their business, and commensurate with the ML/TF risk to which they are exposed.

New areas within the Guidelines includes:

- **Guidelines 2.1.** on determining whether a card, instrument or device is used exclusively to pay for goods or services;
- **Guidelines 3.** on steps to address technical limitations;
- **Guidelines 3.1.** on the interoperability of messaging or payment and settlement systems;
- **Guidelines 4.** on identifying the specific data points to be transmitted as part of the information required under Article 4(1), (2) and Article 14(1), (2) of Regulation (EU) 2023/1113;
- **Guidelines 8.** on self-hosted wallets; and
- **Guidelines 9.** on obligations on the payer's PSP, payee's PSP and IPSPs where a transfer is a direct debit.

The deadline for competent authorities to report whether they comply with the Guidelines will be two months after the publication of the translations into the official EU languages. The amending Guidelines will apply from 30 December 2024. The full Guidance document can be found here.

EBA publishes it's 2024 Report on Payment Fraud

On August 1st 2024, the European Banking Authority (EBA) released its Report on Payment fraud. This report, jointly prepared by the EBA and the European Central Bank ("ECB"), assesses the latest payment data reported to the EBA and the ECB under the Payment Services Directive ("PSD2") and covers semi-annual data reported for the three reference periods H1 2022, H2 2022 and H1 2023. The report focuses on the payment instruments of credit transfers, direct debits, card payments (from an EU/EEA issuing perspective), cash withdrawals and e-money transactions.

Key highlights of the Report include:

- **Fraud Amounts:** Payment fraud in the European Economic Area (EEA) amounted to €4.3 billion in 2022 and €2.0 billion in the first half of 2023;
- **Fraud Values & Volumes:** Most payment fraud in value terms was related to credit transfers and card payments, across all three reference periods analysed, while in volume terms, 7.31 million card transactions using cards issued in the EU/EEA in H1 2023 were fraudulent, while the number for other forms of payment was significantly lower;
- **Strong Customer Authentication ("SCA"):** The report confirms that SCA transactions showed lower fraud rates than non-SCA transactions, especially for card payments.
- **Fraud Losses:** Losses due to fraud are distributed differently among liability bearers depending on the payment instrument used. In H1 2023, payment service users (PSUs) bore 45% and 51% of the losses that arose from card payments and cash withdrawals, respectively; this share was below 25% for e-money transactions. In contrast, PSUs endured more than 80% of total fraud losses for credit transfers.
- **Geographical Dimensions:** the results show that, while most payment transactions were domestic, most card payment fraud (71% in value terms in H1 2023) and a large share of credit transfer and direct debit fraud (43% and 47%, respectively, in H1 2023) were crossborder. A notable share of fraudulent card payments (28% in H1 2023) was thereby related to cross border transactions outside the EEA.

The report notes that, looking ahead, the general outlook with respect to overall payment fraud based on the presented analysis appears stable. The widespread adoption of the Regulatory Technical Standards for SCA and Common and Secure Open Standards of Communication ("CSC") has had a positive effect on reducing fraudulent payments, especially for transactions conducted within the EEA. Nevertheless, it is important for the industry, regulators and consumers to remain alert. Both the EBA and the ECB will continue to closely monitor developments in payment fraud.

You can read the full Report here.

ERPB Working Group Report on fraud related to retail payments

In September 2024, the Euro Retail Payments Board (ERPB) published their final report on fraud related to retail payments. The report outlines recommendations formulated by the working group, which are addressed to both the European Union and national authorities, as well as to all actors along the 'fraud chain'. Working group discussions identified issues considered relevant to provisions of the proposal for a Directive on payment services and electronic money services (PSD3) and of the proposal for a Regulation on payment services in the internal market (PSR) currently under consideration by the EU's co-legislators.

To prevent and mitigate fraud more effectively and across the fraud chain, the working group has identified four 'gamechangers'. For each gamechanger, the working group recommends several actions to be implemented by EU and national authorities, as well as institutions and entities from the private sector. These game changers are:

1. Cross sectoral collaboration & responsibilities;
2. Sharing Fraud insights & data;
3. Supervisory enforcement cooperation at EU level across sectors; and
4. Secure Product design for consumer protection.

Further details on these game changers and well as the activities of the working group can be read here.

UK Financial Crime Updates

13

FCA Review on the Treatment of Politically Exposed Persons

In July 2024, the Financial Conduct Authority (FCA) published results from their review of the treatment of Politically Exposed Persons (PEPs). This review was undertaken following a request from Parliament, as concerns were being raised that FCA regulated firms were not effectively applying the FCA PEP Guidance. The concerns raised included PEPs and Relatives and Close Associates ("RCAs") having to provide a lot of information about their wealth and income, as well as PEPs and RCAs being denied services, respectively because of their status or connection to a PEP. In undertaking this review the FCA looked at how firms apply the definition of PEPs and RCAs to individuals and assessed how firms are set up to take a risk-based and proportionate approach in their management and treatment of UK PEPs and RCAs, in accordance with the FCA Guidance. The FCA also contacted over 1,000 PEPs and received 65 individual responses.

Key findings from this FCA review included:

- Some firms included definitions for PEPs and RCAs that are not in line with the relevant UK regulations and the FCA Guidance;
- Some firms did not have effective arrangements in place to review PEPs and RCAs to ensure the PEP classification remained appropriate after the PEP had left public office;
- A small number of firms did not effectively consider the customer's actual risk in their assessment and rating;
- Despite the need to improve the firms' policies and procedures, customer file testing did not show firms regularly applying excessive enhanced due diligence measures for customers;
- All of the 15 firms were clear that they would not decline products or services to UK PEPs or their RCAs simply because of PEP status;
- Firms need to improve the clarity and detail of communications with PEP and RCA customers;
- Most of the 15 firms needed to improve staff training; and
- Ten of the 15 firms had made changes and improvements following the recent amendment to Regulation 35 (which sets out firms' AML obligations on PEPs under the Regulation) but some needed to update their policies to reflect this legislative development

The FCA identified four actions that all firms need to take

- Review their current arrangements (policies, procedures, controls) for the risk management and treatment of PEPs and RCAs against these findings. Their current arrangements must reflect the legislative position, effective from 10 January 2024, which makes clear that UK PEPs and RCAs should be considered as presenting a lower level of risk if no enhanced risk factors are present;
- Address any gaps they identify in their current arrangements. This includes making any necessary improvements such as updating their policies and procedures, (ensuring these are aligned with the relevant regulations and FCA Guidance) and more practical staff guidance on the risk-based and proportionate approach for the treatment of PEPs and RCAs;
- Make sure that communication with customers is clear and effective when requesting information so that PEPs and RCAs can understand what information is being sought and why the requests are being made. Firms will, where relevant, need to comply with the Consumer Duty requirements to ensure their communications meet customers' information needs, are likely to be understood by customers and enable them to make decisions that are effective, timely and properly informed; and
- Make sure that staff are appropriately trained (through, for example, the use of case studies and other practical guidance) so that the firm's policies and procedures are consistently and effectively applied in line with the regulations and our Guidance.

The full FCA report from this review can be found here.

FATF Financial Crime Updates

FATF Report on Implementation of Standards on VAs and VASPs'

In July 2024, FATF released a report providing their fifth update on jurisdictions' compliance with FATF's Recommendation 15 and its Interpretative Note (R.15/INR.15). This recommendation was updated in 2019 to apply AML/CFT measures to Virtual Assets ("VAs") and Virtual Asset Service Providers ("VASPs"). The report released by FATF also provides updates on emerging risks and market developments relating to the use of VAs for money laundering, terrorist financing and proliferation financing.

The FATF's report finds that:

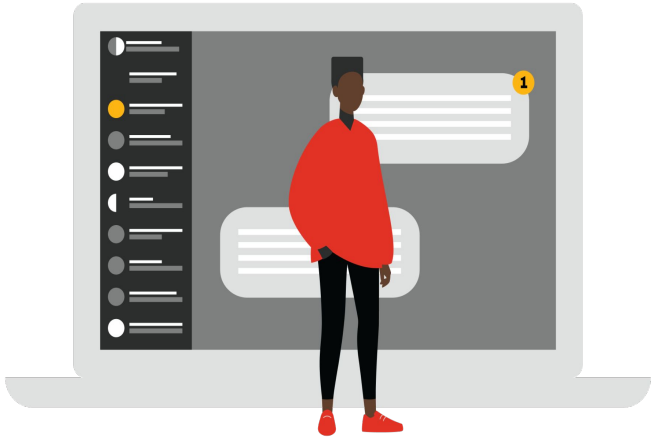
- While some jurisdictions have made progress in putting AML/CFT regulation in place, global implementation is still lagging;
- It is recognised that when focusing on the countries with materially important VA sectors, the picture is better with the majority of these countries having the core measures in place;
- Despite progress made by individual countries, there is still a lot of work to do in order to complete the global system of AML/CFT regulation for the virtual asset sector, and FATF will continue to prioritise closing these gaps;

In relation to the Travel Rule, it is noted by FATF in their report, that jurisdictions have made insufficient progress in implementing the Travel Rule, which is a key AML/CFT measure. Nearly one third of the survey respondents, including some who assessed VA/VASPs as high risk, have not yet passed legislation implementing the Travel Rule.

The FATF has called on all jurisdictions to rapidly implement the FATF's Standards on VAs and VASPs, including the FATF's Travel Rule. The full FATF report can be read here.

FATF Horizontal Review of Gatekeepers' Technical Compliance Related to Corruption

On July 9th the FATF released a report on the Horizontal Review of Gatekeepers technical compliance related to corruption. The FATF has undertaken the Review to assess the current state of play with regards to corruption and AML, and identify areas that FATF members must prioritise for further improvement. This is a deep dive into the actions that FATF members have taken to apply important aspects of the FATF Recommendations to gatekeepers, which covers lawyers, accountants, trust and company service providers, and real estate agents.



The main points of the FATF Review include:

- The FATF notes that on the surface, the Horizontal Review shows positive results - over half of FATF members have scores over 80%. However, these results are less promising when one considers the context and materiality of the seven FATF members falling below the score of 50%. These jurisdictions represent more than half of the world's GDP.
- Although it is a common perception that the legal profession is subject to fewer AML/CFT rules than other gatekeeper sectors, the Horizontal Review found little difference in coverage scores of the four gatekeeper sectors under the scope of the review.
- Some cornerstone obligations of the FATF recommendations fall behind the compliance levels of other obligations. These requirements - conducting customer due diligence, implementing internal controls, and providing a supervisor with adequate powers to conduct risk-based supervision, are essential requirements to address the vulnerability of gatekeepers to money laundering and corruption threats.

The Review emphasized that it is urgent that those FATF members still lagging behind must ensure that gatekeepers are adequately covered in line with the FATF's long standing Recommendations in the area of AML and corruption.

To read the full Review report click here.

How can PwC help you?

Our Financial Services Regulation Team at PwC Ireland have the experience and expertise to provide solutions that have the overarching aim of addressing new and existing financial crime threats. Get in touch to find out more on how we can help you.

Central Bank RMPs focused on AML

PwC can assist firms in navigating the many demands and challenges of addressing and responding to an AML focused RMP with a selection of our services provided below:

- Design and implementation of a RMP response framework, including tracking, monitoring and reporting
- Constructing a Governance framework, that includes management and Board reporting
- Developing risk mitigation planning, implementation, and progress monitoring
- Leveraging the latest technology to assist in assessing risk and data analytics

Target Operating Model

PwC can assist firms in transforming their AML / Financial Crime Target Operating Model through:

- Reviewing your current operating model to identify / address regulatory gaps
- Assessing and advising on the most appropriate technology available to manage your FC risks
- Advising on your 3LOD structure to ensure that all FC activities are operating effectively, efficiently and meeting regulatory expectations;
- Designing Policies, Procedures and Processes to manage FC within your organisation.

AML Remediation Programmes

PwC has vast experience in conducting large scale AML remediation programmes, achieved by:

- Designing a tailored and specific remediation plan, which includes a formalised governance framework and comprehensive resource planning.
- Providing a team of highly experienced and industry focused individuals.
- Assisting clients with the delivery of the programme, including customer outreach and independent quality assurance.
- Assistance with key AML processes, including CDD, Transaction Monitoring and Screening.

AML Risk Mitigation

The appropriate assessment of risk is a key area of focus for the CBI. We can support you to assess and enhance your AML risk assessment process through the review of:

- Your Business Wide Risk Assessment - identification of gaps and opportunities for improvement in AML/CFT methodology
- Your Customer Risk Assessment process - identifying and assessing a comprehensive list of risks making up your customer's risk profile.

FC Technology & Automation

PwC has significant experience in assisting clients with managing and assessing their Financial Crime Technology infrastructure, including:

- The assessment of existing Technology;
- Identification of new FC technology requirements; and
- Support in the implementation of new technology with your organisation.
- Identification of opportunities to introduce automation and Gen AI into your FC & AML processes.

Contact

FS Risk and Regulation - Financial Crime

Sinead Ovenden
Partner - FS Risk & Regulation
E: sinead.m.ovenden@pwc.com

Aoibheann Morgan
Director - FS Risk & Regulation
E: aoibheann.morgan@pwc.com

Ri Drozan
Senior Manager - FS Risk & Regulation
E: irina.drozan@pwc.com

Lauren Cleary
Manager - FS Risk & Regulation
E: lauren.cleary@pwc.com