Q1 2025 - Financial Crime Quarterly Updates

January - March 2025

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 both locally in Ireland and wider at an European and global level.

In Ireland, the CBI published their Regulatory & Supervisory Outlook report for 2025, which contains key Financial Crime insights for regulated firms in Ireland. The Department of Justice also released their latest Terrorist Financing Risk Assessment. At a European level, the EBA released a Consultation paper on proposed Regulatory Technical Standards under the new EU AML Regulatory 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

Innovation and technology in financial crime - remarks by the Deputy Governor, Consumer & Investor Protection

On February 4th 2025, Derville Rowland, Deputy Governor, Consumer and Investor Protection, spoke at the Afore Annual FinTech and Regulation Conference on the topic of "the utilisation of innovation and technology to conduct - and most importantly, combat - financial crime". Ms Rowland outlined that she believes in the potential benefits of innovation and technology for consumers, investors, businesses and society and that she wants to see them realised but acknowledged that this also means that risks must be effectively managed. Some of the key risks highlighted by Ms Rowland include:

- The anonymity of virtual assets can be used to transfer illicit funds quickly and across borders, with criminals increasingly leveraging new technologies to commit fraud, launder the proceeds of crime, and carry out financing of terrorism; and
- The speed at which funds can be moved across borders makes it easier for criminals to exploit the financial system.

Ms Rowland noted the importance of the new EU AML Package and highlights that it is "by design technology neutral". Ms Rowland outlined that how firms comply with the rules is up to them, via traditional AML/CFT compliance programmes or by using regtech tools. What is essential is that the means used are effective, and that such effectiveness can be demonstrated to supervisors. She notes that the EU, through this AML package are addressing some of the emerging risks, including:

- AI is acknowledged under the package, with an obligation on firms to ensure that human oversight is applied to decisions proposed by AI tools that may impact customers in certain areas;
- Details of Virtual IBANs which are linked to other payment accounts will have to be recorded in member states' Bank Account Registers. This will allow law enforcement to trace any funds being moved by such Virtual IBANs; and
- The package introduces the concept of Information Sharing Partnerships. Through these, credit and financial institutions will be enabled to share information relating to high risk customers, subject to important guardrails including data protection assessments.

In relation to information sharing, Ms Rowland sees this as a "real game-changer" and notes that tech solutions, including tools which can allow information to be shared between financial institutions in a manner that complies with GDPR, will be essential here.

Ms Rowland also highlighted the importance of effective technological solutions when addressing sanctions (which the new EU AML Package is forward looking on) - Ms Rowland notes that the use of screening tools will be imperative for firms seeking to protect themselves from the possibility of breaching sanctions.

Outside of technology advances, Ms Rowland welcomes the fact that The EU and member states have started thinking about fraud and money laundering more holistically, rather than two silos to be tackled independently. She notes that the CBI is approaching AML, fraud, and sanctions through the lens of financial integrity of the system, building out a more integrated supervisory framework to look at risk in a more holistic way. The CBI wants to take a whole of sector, rather than a piecemeal approach, and so very much support EU thinking in this area. Work already under way in this area in the EU includes PSD3 and the Payment Services Regulation, the EU's Markets in Crypto Assets Regulation and the amended Fund Transfer Regulation.

Aligned to the topic of Innovation and technology, Ms Rowland provided an update on the CBI's new Sandbox initiative, nothing that while they are still at an early stage of the Programme, some of the key areas of focus include the use of AI, machine learning and pattern recognition to detect and prevent fraud and the use of technology to enable data sharing without compromising sensitive information.

Ms Rowland concluded her speech, noting that *"The reality is that no piece of legislation can contemplate every financial crime risk or typology or close every loophole. We can't wipe out financial crime – any more than we can wipe out car theft, shoplifting or burglary. But what we can do is to become as effective as possible at reducing its impact".*

You can read the full speech from Ms Rowland here.

Central Bank of Ireland publishes new data on Irish payment fraud

On January 24th 2025, the Central Bank of Ireland ("CBI") published a new "Behind the Data" (BTD) paper on Irish payment fraud statistics. The BTD paper features insights on payments fraud in 2022 and 2023 in Ireland across primary payment methods including credit transfers, card payments, e-money and direct debits. It also examines how fraud varies across these payment methods, which types of frauds are most common, and how much money is lost to fraud.

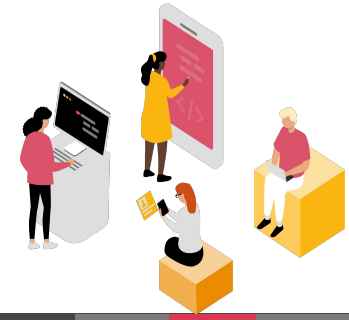
The findings of the BTD paper reveal that although fraud is growing in Ireland, Irish fraud rates remain below EU averages across most payment methods with the exception of card payments.

Some of the key data published in the BTD paper includes:

- Around 98% of card payment fraud by value was accounted for by 'issuance of payment orders by the fraudster'. This occurs where fraudsters use stolen cards, accounts or personal information for a payment;
- Payer manipulation fraud rose from 27% in the first half of 2022 to 42% by the end of 2023;
- Credit transfer fraud amounted to €70m in 2023, with 24,000 transactions;
- The total value of fraudulent payments rose by 26% in 2023, increasing to €126m from €100m in 2022;
- The rate of fraud in Ireland as a share of all transactions is low. By value the rate is 0.001%, and by volume the rate is 0.01%;
- Card payment fraud rate is by far the highest among payment method, with 0.034% of card payments by value being fraudulent;
- Around 50% of fraud in electronic payments by value were not authenticated via Strong Customer Authentication, amounting to €52 million in 2023;
- Online card payments made up 86% of the total value of card fraud in 2023, amounting to €37.4m
- The value of money remittance frauds has more than tripled from €2.5m in 2022 to €8.2m in 2023; and
- Approximately 60% of the total value of fraud across 2022-2023 involved cross border payments, amounting to € 77m in 2023 and € 64m in 2022.

The CBI notes that "combating fraud in the financial system is a priority for the Central Bank, working closely with law enforcement, other State agencies and peer regulators. In 2024, the Central Bank launched a campaign to help consumers avoid scams, with further information available for this campaign on their website.

You can read the full BTD paper here.



Publication of Ireland's latest Terrorist Financing Risk Assessment

On March 18th 2025, the Department of Justice published Ireland's latest Terrorist Financing (TF) Risk Assessment (RA), which is reviewed every 2 years. The Financial Action Task Force (FATF) requires each country to identify, assess and understand the terrorist financing risks it faces in order to put mitigation measures in place and disrupt terrorist networks. This latest risk assessment from Ireland will be used by a range of departments and agencies to identify areas where measures need to be put in place. The RA notes that the character 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. It also notes that within both of these categories, a further distinction must be made between the assessed threat of an act of terrorism within Ireland and the risk of terrorist financing (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.

Domestic Assessment of risk of TF: The risk assessment carried out by Ireland finds that the costs associated with domestic terrorist acts – including those taking place in Northern Ireland and Great Britain – are relatively small for the most part and therefore the material used in such acts can often be procured through the activist's own personal means or direct theft. 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. It is noted that 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. It is also considered that the success of An Garda Síochána over the years has significantly degraded the capacity of Republican paramilitary groups to finance their operations and it is considered that such groups do not have significant reserves.

International RA: 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. However, the RA notes that the threat to Ireland is not assessed to be comparable to that which exists in other European jurisdictions. It is assessed that the current risk of an attack in Ireland from this source is moderate. The RA also notes that there is the possibility, albeit currently assessed to be low, that Ireland could be used as a base from which attacks could be planned, etc. 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 factors within Ireland for support to activities outside Ireland.

Using methodology deployed by the 2022 EU Supranational Risk Assessment (SNRA), the TF RA provides detailed analysis on sector-specific risks. Some Areas of the Financial Sector identified with Significant/ Very Significant risk includes:

- **Very significant:** Retail banking sector, E-money, Crypto-assets
- **Significant/Very significant:** Transfers of funds and money remittance
- **Significant:** Illegal transfers of funds — Hawala, Payment services, Consumer credit and low-value loans

Outside of the Financial Sector, the TF RA also provides an assessment of the TF risks in a wide range of other sectors, including Non-profit organisations, gambling sector products and free-trade zones.

You can read the full risk assessment here.

Central Bank of Ireland - Regulatory & Supervisory Outlook Report 2025

In February 2025, the CBI published their Regulatory & Supervisory Outlook report which sets out the key priorities of the CBI for 2025/26. These priorities are aligned with the corresponding priorities of the European System of Financial Supervision and ECB Banking Supervision. Within this report, the CBI called out six key supervisory priorities and expectations of firms, which continue to be as set out in the 2024 report:

- **Priority 1:** Proactive risk management and consumer-centric leadership of firms;
- **Priority 2**: Firms are resilient to the challenging macro environment;
- **Priority 3:** Firms address operating framework deficiencies;
- **Priority 4:** Firms manage change effectively;
- **Priority 5:** Climate change and net zero transition are addressed; and
- **Priority 6:** The Central Bank enhances how it regulates and supervises.

From a Financial Crime perspective, the CBI plans to:

- take an increasingly holistic approach to fulfilling their remit in connection with financial crime and market integrity. The expectation is that firms are developing and implementing preventative measures to mitigate fraud;
- engage with technology providers to introduce protections to help mitigate against the risks to the public from scams and fraud;
- make a material contribution to the work of the Anti-Money Laundering Authority (AMLA) which will become administratively operational in 2025; and
- deliver on the first thematic Innovation Sandbox Programme focusing on combating financial crime and expanding the programme to continue to support innovation while safeguarding the integrity of the financial sector.

In relation to Priority 6, as part of their enhancements to regulation and supervision, the CBI notes that one of the areas they are focusing on is prioritising work around FC affecting consumers of financial services through fraud or the laundering of the proceeds of crime.

The report from the CBI provides an overview of the trends, risks and vulnerabilities that are considered from a Sectoral perspective. In relation to FC, the Report found that:

- **Banking Sector:** Retail banking continues to be one of the main access points to the financial system, rendering banks operating in this area particularly attractive for ML/TF - While AML/CFT control frameworks are in general mature, it is imperative that firms' control frameworks continue to evolve in line with rising risk levels, in particular, to have more effective use of technology.
- **Payment and E-Money Sector:** Given the high volume of transactions and international reach of the sector, and complex operating models, this sector has an inherently higher risk that it is used as a vehicle for ML/TF & FC. The CBI notes shortcomings in the understanding of these risks and that controls are not as robust as they should be and not commensurate with the level of risk exposure.
- **Credit Union Sector:**, the current inherent risk of ML/TF in the sector remains at a medium-low level, however, as credit unions expand their product and service offerings, this may expose them to an increase in ML, TF and FC risk.
- **Securities Markets Sector**, a lack of transparency in the crypto asset sector, including ownership, may attract more users with illicit intentions than other asset classes where ownership is more transparent. This could cover money laundering, the financing of terrorism and as a ransom payment for cyberattacks. It is noted that some firms in this sector lack strong controls and understanding of the risks.
- **Funds Sector:** The CBI has identified AML control deficiencies in the areas of AML/CFT risk assessments, governance and oversight, customer due diligence processes and suspicious transaction reporting process and procedures. These areas will continue to be a focus of the Central Bank and firms will be subject to on-going scrutiny and assessment of the robustness of these controls.

In closing out the report, the CBI highlights some key regulatory initiatives, which includes the AML/CFT Legislative package.

You can read the full report here.

Ireland's first cross-sector Anti-Fraud Forum chaired by BPFI to strengthen national response to FC

On Wednesday 19th March 2025 the Banking & Payments Federation Ireland (BPFI) hosted the inaugural meeting of Ireland's new Cross-Sector Anti-Fraud Forum, bringing together key stakeholders from across the financial services sector, telecommunication service providers, online platforms and their respective regulator along with government and An Garda Síochána, to enhance collaboration in the fight against fraud.

This forum was established as a key action under the National Payments Strategy, published by the Department of Finance in 2024. It is noted that the Forum represents a major step forward in tackling the rising threat of financial crime through shared intelligence, coordination, and collective action.

The BPFI, in launching the forum, notes that they have played a central role in shaping this initiative, working closely with industry partners and Government to ensure a robust framework for fraud prevention, detection, and disruption. The BPFI will chair the Forum for the initial period of 2.5 years after which it will rotate to other industries on the forum.

Speaking ahead of the meeting, Niamh Davenport, Head of Financial Crime, BPFI and Chair of the Anti-Fraud Forum said: "The establishment of this Forum marks a significant milestone in Ireland's approach to tackling fraud. Fraud is an ever-evolving challenge, with criminals exploiting new technologies and cross-border tactics. By bringing together all the key players around one table, this Forum will help drive a more unified and proactive response to emerging threats. Criminals do not operate in silos, and neither can we. By working together across sectors, we can better protect consumers, businesses, and the integrity of the financial system."

The Forum is set to develop a cross-sector charter and meet regularly to exchange information on evolving trends, coordinate actions, and drive key initiatives that strengthen fraud defences across all sectors.

European Financial Crime updates

EBA's recommendations on tax integrity and dividend arbitrage trading schemes

On February 6th 2025, the EBA published a Peer Review assessing the effectiveness and degree of supervisory convergence of issues relating to tax integrity and dividend arbitrage trading schemes following the implementation of its 2020 Action plan on dividend arbitrage trading schemes. The action plan aimed to clarify that supervisors, while not responsible for investigating tax crimes, have responsibility for ensuring that financial institutions have systems and controls in place to manage tax crime risks. The Peer Review sampled six national prudential authorities and supervisors on anti-money laundering and countering the financing of terrorism (AML/CFT) to see how they integrated tax integrity into their risk-based supervisory work.

The Peer Review focuses on the responsibilities assigned to AML/CFT and prudential supervisors, mainly to ensure that financial institutions have systems and controls in place to manage tax crime risks. The Report does not look at or comment on the effectiveness of the national frameworks in place to identify or investigate tax crimes which are beyond the responsibility of AML/CFT and prudential supervisors. The Report sets out its findings based on four benchmarks:

- the effectiveness of integration of tax integrity into risk-based AML/CFT supervisory work on credit and financial institutions;
- the effectiveness of integration of tax integrity into sectoral and institution-specific ML/TF risk assessments;
- the effectiveness of arrangements for reviewing the due consideration of tax integrity in institutions' internal governance arrangements;
- the effectiveness of consideration of tax integrity in the assessment of the reputation, honesty and integrity of members of the management body and key function holders.

The peer review found that most of the supervisors reviewed largely or fully applied the benchmarks assessed, hence supervising these areas well overall. However, the detail underlying the assessments revealed some specific areas for improvement and follow-up measures. For example, two supervisors were assessed as only partially applying the expectations concerning supervisory activities covering tax integrity from an AML perspective.

The EBA identified general and individual follow-up measures, which will help further build consistency and effectiveness in supervisory outcomes across the EU and to limit the financial system's exposure to illegal tax schemes and other tax evasion.

You can read the full EBA Report here.

EBA & ESMA Analysis of recent developments in Crypto-Assets

In January 2025, the European Banking Authority (EBA) and the European Securities and Markets Authority (ESMA) published a joint report on recent developments in crypto-assets. The report addresses specific elements covered by Article 142 of MiCAR and has been informed by extensive research on DeFi and crypto lending, borrowing and stalking.

In relation to AML, the report finds that DeFi protocols present significant risks of ML/TF, with flows on decentralised exchanges representing 10% of spot crypto trading volumes globally. This is mainly due to the current absence of adequate AML/CFT controls, which means that users can transact in practice without being identified and verified. The risk is increased due to the cross-border nature of transactions as the funds or crypto-assets from potentially illegitimate sources can be transferred via DeFi without any obligations on the protocols to perform AML/CFT checks on such funds or crypto-assets and report them to Financial Intelligence Units.The report identifies some initiatives to apply KYC in DeFi protocols.

In highlighting potential risks that are common to lending, borrowing and stalking, the report notes that ML/TF risks associated with lending, borrowing and staking (regardless of whether these services are centralised or decentralised) are broadly the same as those associated with crypto-assets in general and with credit activity in particular. These risks include:

- Anonymity or pseudonymity of customers;
- Transactions involving illegitimate funds or crypto-assets;
- Unclear purpose of the transaction; and
- Exposure to high ML/TF risk jurisdictions

It is acknowledged in the report that the ML/TF risks can be reduced where lending, borrowing or staking services also involve some of the CASP services regulated under the MiCAR or other applicable frameworks and the providers are therefore required to perform adequate CDD checks. However, the report concludes that while CDD checks may give some level of protection against ML/TF, their impact may often be limited. As crypto-assets are continuously transferred between users and DeFi protocols, it may be difficult or, in some cases, impossible, to establish the legitimacy or true ownership of funds or crypto-assets used in transactions.

The report can be read in full here.

EFIPPP Practical Guide for Operational Cooperation between Investigative Authorities and Financial Institutions

In January 2025, Europol Financial Intelligence Public Private Partnership (EFIPPP) published a practical guide for Operational Cooperation between Investigative Authorities and Financial Institutions. The guide outlines that although cooperation between investigative authorities and financial institutions can occur in a variety of ways, the new EU AML/CFT framework introduces a legal basis that could significantly increase the potential for investigative authorities and FIUs to cooperate with obliged entities. Specifically, Article 75 of the new Regulation (EU) 2024/1624 introduces the concept of 'partnerships for information-sharing'. Furthermore, Article 93 of the new Regulation (EU) 2024/1620 authorises the new Anti-Money Laundering Authority to set up cross-border partnerships for information sharing, and to participate in partnerships for information sharing established in one or across several Member States.

The guide covers a range of topics, including:

- Where public-private cooperative mechanisms already exist in Europe (including the Irish Joint Intelligence Group);
- The objectives of cooperation;
- Benefits and added value of cooperative mechanisms;
- Methods and scenarios of cooperation between investigative authorities and financial institutions;
- Fundamental conditions of cooperation; and
- General rules of cooperation

The full guide can be accessed here.

EBA Consultation Paper on Proposed RTSs

On 6th March 2025, the EBA issued a consultation paper on 'Proposed Regulatory Technical Standards (RTS) in the context of the EBA's response to the European Commission's Call for advice on new AMLA mandates'. This consultation has been issued as the EBA received a Call for advice (CfA) from the European Commission in March 2024 on certain draft regulatory technical standards (RTSs) under the new EU AML/CFT Framework. The EBA's response to the CfA will inform the work of the new AML/CFT Authority (AMLA). The CfA covers the following mandates:

- The mandate, under Article 40(2) of Directive (EU) 2024/1640, to develop draft RTS on the assessment and classification of the inherent and residual risk profile of obliged entities and the frequency at which such profile must be reviewed;
- The mandate, under Article 12(7) of Regulation (EU) 2024/1620 (AMLAR), to develop draft RTS on the risk assessment for the purpose of selection for direct supervision;
- The mandate, under Article 28(1) of Regulation (EU) 2024/1624 (AMLR), to develop draft RTS on customer due diligence (CDD);
- The mandate, under Article 53(10) of AMLD6, to develop draft RTS on pecuniary sanctions, administrative measures and periodic penalty payments.

The consultation paper issued by the EBA in March includes the EBA's proposals for the draft RTSs mentioned above. They address supervisors and obliged entities that fall within the EBA's remit. When putting together its proposals, the EBA was guided by the principles of a proportionate, risk-based approach that can be applied effectively by financial institutions and their AML/CFT supervisors and is conducive to limiting the cost of compliance where possible.

Next Steps:

The EBA invites comments on all of the proposals put forward in the Consultation paper, and in particular on the specific questions summarised in the paper. Responses are due by June 6, 2025. The EBA will consider feedback to this consultation when preparing its response to the European Commission, which it will submit on 31 October 2025.

You can read the EBA's full consultation paper here.

UK Financial Crime Updates

FCA review finds gaps remain in wholesale brokers' money laundering defences

In January 2025, the FCA published findings from its review of wholesale brokers. Through this review, the FCA found that wholesale brokers need to enhance their systems, controls, risk awareness and training to guard against money laundering.

While the regulators review focused on wholesale brokers because of the important role that they play in capital markets in facilitating deals, the regulator also engaged with other market participants to understand wider risks, issues and good practice, recognising that collaboration with and across industry is essential to delivering real improvements. This report is meant to assist any firms involved in the capital markets to improve their controls and prevent financial crime.

The Report found that good progress has been made since the FCA's Thematic Review in 2019, including with customer risk assessments, onboarding processes, governance and oversight, and collaboration between trade surveillance and transaction monitoring teams.

However, the FCA identified areas where firms needed to improve to better protect against money laundering, including:

- an underestimation of the risks of money laundering firms are exposed to;
- over-reliance on others in the transaction chain completing appropriate due diligence checks on customers
- limited information sharing between firms; and
- insufficient awareness of money laundering through the markets suspicious activity reports glossary code.

The FCA concluded that it will continue to work closely with firms, industry and law enforcement to improve understanding and sharing of information about emerging risks and to encourage greater innovation by firms with transaction monitoring.

You can read the full publication here.

FCA: Use of the National Fraud Database and Money Mule Account Detection Tools

In January 2025, the FCA published key findings from their review of payment services and account providers' use of the National Fraud Database (NFD) and a money mule account detection tool to tackle risks associated with money muling activities. The FCA highlights findings from the National Crime Plan 2 (2023 - 2026) and the Fraud Strategy, which identifies money mules' integral role in moving the proceeds of fraud and enabling other crime types. The findings note that this practice can also result in serious consequences for those persuaded or duped into allowing criminals to move money through their account. This underlines the importance of disrupting mule activity to protect the public.

With this in mind, the FCA data indicates that a total of 194,084 money mules were offboarded by 25 firms between January 2022 and September 2023. Of these off-boarded money mules, only 37% were reported to the National Fraud Database (NFD).The FCA highlights that using the NFD effectively, together with detection tools designed to trace the proceeds of fraud across payment networks, is critical in tackling mule activity.

The FCA notes that these findings should be read in conjunction with their previously published findings, in November 2023, where they shared their expectation for firms to strengthen their controls during onboarding, improving transaction monitoring to detect suspicious activity involving money mules, and to robustly address the associated risks.

While the FCA noted positive findings from their review, such as the fact that where firms are filing customers' details to the NFD, the expected high evidential standards were met, supported by thorough investigations. However, areas for improvement and key challenges were also highlighted by the FCA in their findings. One of the key challenges highlighted was that firms find it challenging to demonstrate conclusively whether the customer willingly participated in money mule activities.

In relation to the FCA review of firms' use of a money mule account detection tool, the FCA were informed by firms that the tool's effectiveness increased when corroborated by additional supporting information. As a result, they do not treat alerts raised through the detection tool as a clear indicator of muling activity on their own.

In terms of next steps the FCA outlined that they:

- Will continue to directly engage with the firms included in this review to ensure they consider these findings to enhance their overall systems and controls for fraud;
- Expect all other payment services and account providers to consider their own systems and controls against the FCA findings. It is vital that firms have a proactive approach to identifying and swiftly remedying any weaknesses in their response to tackling the risks posed by money muling; and
- Expect firms to have strong and effective systems and controls to mitigate the risk of money mules. Crucially, firms must consistently keep under review their detection and monitoring methodologies, prioritising the identification of money mule activity, alongside educating consumers about the risks of money muling.

You can read the full publication here.

Dear CEO Letter: FCA priorities for payments portfolio firms

In February 2025, the FCA published a Dear CEO letter, setting out their priorities for firms supervised by the FCA in the payments portfolio sector. The letter set out three priority outcomes:

- **Outcome 1:** Effective competition and innovation to meet customers' needs, characteristics and objectives.
- **Outcome 2:** Firms do not compromise financial system integrity.
- **Outcome 3:** Firms keep customers' money safe.

Within Outcome 2, one of the focus areas to enhance financial financial system integrity in the payments sector is Financial Crime. The FCA notes that reducing and preventing financial crime to instill trust and confidence in the market, which is essential for innovation, competition, and growth, is a commitment in the 2024/2025 business plan of the FCA and a key theme in their upcoming strategy.

The FCA notes that they have been encouraged by some firms significantly enhancing their financial crime controls. However, there is still more for firms to do. It remains the case that weaknesses in some firms' governance, oversight, and systems and controls make them a target for bad actors and risks the loss of critical services for customers. The FCA requests that firms ensure that their governance arrangements and systems and controls, including reporting mechanisms, are effective and proportionate to the nature, scale, and complexity of their business, and the risks to which it is exposed. They also draw readers attention to two recently published documents - a Dear CEO Letter regarding the PSR's reimbursement requirements for APP fraud carried out through the Faster Payments System and CHAPS and Guidance on the recently introduced payment delays legislation.

The full Dear CEO Letter can be read here.

FCA Launches new 5-year Strategy

In March 2025, the FCA launched a new 5-year strategy “to deepen trust, rebalance risk, support growth and improve lives”. The strategy focuses on 4 priorities, namely:

- Be a smarter regulator;
- Support sustained economic growth,
- Help consumers navigate their financial lives
- Fight financial crime

In relation to Financial Crime, the FCA notes that they will be focusing on those who seek to use the fact they are regulated to do harm. It will go further to disrupt criminals and support firms to be an effective line of defence.

In outlining how they will achieve this aim, the FCA notes that they will continue to police their complex remit and work with partners to disrupt crime, including scams. They will draw on all the tools at their disposal to get the best outcome they can, from public warnings, formal requirements on firms, civil action or criminal prosecution. They also note that they will work with those firms who they know want to play their part in tackling crime, while continuing to act against those through which criminal cash finds its way into the system.

The full FCA 5-Year Strategy can be accessed here.

FATF Financial Crime Updates

Outcomes FATF Plenary February 2025

In February 2025, delegates from the FATF's Global Network of over 200 jurisdictions and observers from international organisations participated in three days of discussions on key money laundering, terrorism financing and proliferation financing issues. Some of the key items discussed and agreed by the FATF Plenary included the following:

- **Jurisdictions under increased monitoring:** the FATF added Lao People's Democratic Republic and Nepal to the list of jurisdictions subject to increased monitoring.
- **Jurisdictions no longer under Increased Monitoring:** Philippines has completed its Action Plans to resolve the identified strategic deficiencies within agreed timeframes and will no longer be subject to the FATF's increased monitoring process.
- **Financial Inclusion and the Risk-Based Approach:** Following a public consultation which gathered more than 140 responses, members agreed to revise the FATF Standards to better support financial inclusion, recognising that around 1.4 billion people around the world still do not have a bank account. Recommendation 1 aims to ensure countries apply a risk-based approach to their anti-money laundering and counter-terrorist financing and proliferation financing measures. The changes will encourage financial institutions applying simplified measures where risks are lower, and thus facilitating people's access to financial services.

Public Consultations:

- **Risk Based Approach:** To embed the changes to Recommendation 1 to support a risk-based approach and financial inclusion, the FATF is working on new guidance that will equip policy makers and regulators with practical examples to encourage widespread adherence to the changes. The FATF invites feedback on this guidance so that the public and private sectors are best able to implement a risk-based approach.
- **Payment Transparency:** FATF also agreed to consult on potential revisions to its Recommendation 16 on payment transparency which would improve standardisation and quality of originator and beneficiary information in payment messages. The FATF seeks the broadest range of views as it aims to support the use of new technologies without compromising defences against illicit finance.
- **Complex Proliferation Financing and Sanctions Evasions Schemes**: FATF seeks input on its work to understand Complex Proliferation Financing and Sanctions Evasions Schemes. FATF will seek information on best practices and challenges on identifying, assessing, understanding and mitigating Proliferation Financing risk. The public consultation will also seek views on how the FATF can support the private sector to meet their CPF obligations

Further information on the above topics and more can be read **here.**

FATF Annual Report 2023-2024

On January 31st 2025, the Financial Action Task Force (FATF) released its Annual Report for 2023-2024 which outlines the work completed by the FATF to prevent the abuse of the international financial system, and strengthen its foundations for sustainable and more inclusive economic development. The Report highlights the significant progress made by the FATF in its fight against financial crime, including:

- **Strengthening global compliance with the FATF standards** – driving preparation for the next round of mutual evaluations, which will be more timely, but also more risk-based, and with a greater focus on effectiveness; and agreeing a more risk-based criteria for identifying countries with strategic weaknesses in the next round;
- **Transparency and beneficial ownership** – improving global transparency standards and supporting countries with guidance and training on preventive measures, leading to numerous countries committing to implement beneficial ownership registries;
- **Amendments to the FATF Standard on Non-Profit Organisations (NPO)** - ensuring that measures to protect and safeguard the NPO sector are targeted and proportionate and that governments do not suppress civil society through overapplication of the FATF standards;
- **Responding to risks to the Global Financial System** – a continued focus on identifying emerging and priority risks, including reports on the cyber-enabled fraud landscape and the exploitation of crowdfunding platforms for terrorism financing, as well as analysis on ransomware and on corruption through the misuse of citizenship and residency by investment schemes;
- **Asset Recovery** - a substantial shift in the focus on asset recovery globally, with the FATF adopting changes to its international standards on asset recovery for the first time since its creation, and working in close partnership with INTERPOL to support operational application; and
- **Virtual assets** – for the first time, publishing a list of jurisdictions with materially important virtual asset service provider (VASP) activity and the steps they have taken to encourage and implement global implementation of the FATF's requirements.

FATF outlined in their report activities completed in 2023-24, including:

- Undertaken two Public Consultations and one targeted consultation to consider a wide range of views in making sure the Standards remain relevant and pragmatic;
- Updated five of the FATF Recommendations and published two Guidance Papers to ensure practitioners have a strong toolkit to more effectively combat financial crime; and
- The FATF actively engaged with its stakeholders to raise awareness about the requirements of the FATF Recommendations, seek input or contribute to collaboration on common projects.

As noted in the annual report, the incoming FATF Presidency will prioritise the following work to support the Strategic priorities for 2024-2026:

- Promote the risk-based implementation of the Standards under the principles of proportionality particularly those that can contribute to advance financial inclusion;
- Ensure a successful start to the new round of assessments;
- Strengthen the cohesion within the Global Network by continuing to foster transparency and inclusiveness;
- Support effective implementation of revised FATF Standards with a focus on the recently strengthened standards on asset recovery, beneficial ownership and virtual assets; and
- Continue efforts to increase and update understanding of terrorist financing and proliferation risks to prevent and combat these activities

You can read the full FATF report here.

Global Financial Crime Updates

Egmont Group Executive Secretary's Speech at the No Money for Terror Conference

In February 2025, at the ministerial conference of No Money for Terror in Munich, the Egmont Group Executive Secretary, Jerome Beaumont delivered a speech highlighting the critical role of Financial Intelligence Units (FIUs) in combating terrorism financing. The Executive Secretary emphasised the importance of multilateral information exchange and the innovative responses needed to address emerging risks posed by technological advancements.

Key points from the speech includes:

- **Technological Challenges:** Virtual assets can be misused to recruit individuals, move funds anonymously, and finance operations through the dark web. FIUs are pivotal in detecting suspicious patterns and tracing illicit flows;
- **Propaganda and Financing:** Terrorist organisations use sophisticated online campaigns to inspire extremism and spread fear. FIUs, with advanced analytical tools, can identify emerging trends and collaborate with the private sector to disrupt these dark networks; and
- **Public-Private Partnerships (PPPs):** Enhancing early sharing of intelligence through PPPs enables financial institutions to detect and disrupt threats before they materialise. These partnerships also help uncover links in the aftermath of attacks.

Mr. Beaumont also promoted the Egmont Centre of FIU Excellence and Leadership (ECOFEL) as a crucial program under the Egmont Group. ECOFEL enhances FIU capabilities through training, research, and technical assistance. By fostering the development of cutting-edge analytical techniques and promoting best practices, ECOFEL equips FIUs to tackle modern financial crimes effectively. It also emphasises multilateral cooperation, bringing together experts and practitioners from around the globe to build a robust network dedicated to safeguarding financial systems.

You can read the full speech 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