



# Q4 2024 - Financial Crime Quarterly Updates

October - December 2024





# 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.

A significant amount of activity happened across the EU in Q4 2024, with a range of Guidelines, Reports and Consultation papers published. This included detailed guidelines on internal policies, procedures and controls to ensure the implementation of union and national restrictive measures and the publication of a very informative fact sheet covering the prevention of money laundering and terrorism financing in the EU's Crypto Assets Sector.

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

1	Irish Financial Crime Updates	03
2	European Financial Crime Updates	06
3	UK Financial Crime Updates	16
4	FATF Financial Crime Updates	19
5	How can PwC help you	24





# Irish Financial Crime Updates





## BPFI Paper: PSR policy recommendations

On November 7th 2024, representatives from the Retail Banks in Ireland joined the Banking & Payments Federation Ireland (BPFI) for a series of important meetings with the European Commission, EU Member State Officials and MEPs on the EU's new Payment Services Regulation (PSR).

Aligned to these meetings, a paper was published titled "A cross sectoral approach to fraud prevention: PSR policy recommendations". Within this paper the BPFI emphasised that tackling the growing trend of payment fraud is critical to protecting consumers and ensuring continued confidence in the payments system. This is especially important as the financial services sector becomes more digital, and the types and methods of fraud become more complex and sophisticated

The BPFI also notes that it is important that policymakers look to take a "whole of sector" approach to the prevention of fraud, considering that the majority of new payment fraud originates online. The BPFI believes that European policymakers should look at further ways to boost fraud prevention, while strengthening the protections around automatic refunds to avoid risks of moral hazard. Specifically the BPFI would recommend the following adjustments to the initial proposal on the draft PSR:

- Include a requirement on all electronic communication providers to verify with national competent authorities that ads promoting financial services companies or products are authorised.
- Require telecom operators to prevent scam text messages or calls by implementing advanced security technologies and protocols, similar to certain Member State requirements.
- Ensure that the definition of authorisation leads to legal certainty, irrevocability, and predictability for payment transactions.
- Examine a shared liability regime based on levy contributions from electronic communication providers

The BPFI outlines that there are still challenges with the proposals given the impact fraud can have on consumers and while progress has been made during the discussions, they believe greater attention needs to be placed on fraud prevention more broadly.

You can read the BPFI position paper on the new Payment Services Regulation [here](#).





## DOF Unveils Vision for 2030: A New Era of Market Resilience and Transparency

On October 22nd 2024, the Department of Finance (DOF), led by Minister Jack Chambers, published the Funds Sector 2030 report titled "A Framework for Open, Resilient and Developing Markets." In producing this report, a review was undertaken by the DOF, with the objective of ensuring that Ireland maintains its leading position in asset management and funds servicing; and that the framework for the sector is resilient, future-proofed, supportive of financial stability and a continued example of international best-practice.

From an AML perspective, the report focused on AML and transparency concerns in relation to Special Purpose Entities (SPEs). Within the report, it is noted that SPEs have been criticised for their complexity and vulnerability to potentially being exploited for ML purposes, sanctions evasion or other offences. The report notes that the Review Team welcomes the developments that have taken place throughout the review period to strengthen the EU AML/CFT regime, including requirements which are relevant to, or apply to, SPEs. These developments include:

- Article 52 of the new AML Directive (EU) 2024/1640 will require self-regulatory bodies (many of whom play an important role in the establishment and operation of SPEs - accountants, notaries, solicitors, etc.) to be subject to oversight by a public authority, to ensure the self-regulatory bodies are conducting adequate and effective supervision, to issue guidelines and, if necessary, to compel the production of information and to issue instructions;
- SPEs are also subject to beneficial ownership requirements, which will continue to form part of the AML package, and have been reviewed in response to challenges which have arisen since the requirements were first introduced; and
- The establishment of the new EU AMLA is a positive development in the enhancement of oversight of all financial services firms and structures such as SPEs (where relevant).

However, the report also notes that additional measures could be implemented to reduce potential ML/TF risks, including:

- Further work to better understand ML/TF risks in the SPE sector and support the development of targeted legislative measures both domestically and at European level;
- To increase transparency in the SPE sector, the Review Team recommends that the DOF and other relevant Departments and agencies introduce the new EU AML package into Irish Law as a priority and ensure its implementation with those Departments/Agencies; and
- To further enhance transparency, the Review Team recommends that legislation be progressed to enable Revenue to publish a list of SPEs availing of the Section 110 regime, including the name of the entity, with the list updated at regular intervals.

You can read the full Funds Sector 2030 report [here](#).





# European Financial Crime updates





## European Parliament approves Chair of EU AMLA

On December 18th 2024, Members of the European Parliament supported Italian candidate Bruna Szego's appointment as Chair of the EU Anti-Money Laundering Authority (AMLA).

Ms Szego, who currently leads the anti-money laundering supervision and regulation unit at the Bank of Italy, received 569 votes in favour, 20 against, and 61 abstentions.

Based in Frankfurt, the new EU AMLA is tasked with coordinating the actions of national financial intelligence units and directly overseeing selected risky financial entities present in multiple member states.

### Next Steps:

To be appointed as AMLA Chair, Ms Szego still needs the support of a qualified majority in the Council.

The official press release from the European Parliament can be accessed [here](#).





## EBA: Guidelines on internal policies, procedures and controls to ensure the implementation of restrictive measures

On November 14th 2024, the EBA published a new set of guidelines on internal policies, procedures and controls to ensure the implementation of union and national restrictive measures.

- The Guidelines set common EU standards on the governance arrangements and the policies, procedures and controls that financial institutions should have in place to be able to comply with restrictive measures;
- Two sets of guidance notes are contained in the document - one is aimed at all institutions within the EBA's supervisory remit and one is aimed specifically at Payment Service Providers and Crypto Asset Service Providers;

Outlined below is an overview of the obligations arising from these two sets of Guidance notes. Further detail is also provided within the general guidelines on the role of the management body in both its Supervisory Function and Management Function, as well as the role of senior staff members in charge of compliance with restrictive measures.

Guidelines EBA/GL/2024/14 provide that financial institutions should:	Guidelines EBA/GL/2024/15 provide that PSPs and CASPs that carry out transfers of funds or crypto-assets should:
1. Put in place, implement and maintain up-to-date policies, procedures and controls for compliance with restrictive measures;	1. Choose a screening system that is adequate and reliable to comply effectively with their restrictive measures obligations;
2. Have a sound governance structure where responsibility for compliance with restrictive measures is clearly allocated;	2. Define the dataset to be screened against restrictive measures adopted by the EU on the basis of Article 29 TEU or Article 215 TFEU and, where relevant, national restrictive measures;
3. Carry out a restrictive measures exposure assessment, which should inform institutions' decision on the types of controls and measures they need to apply to comply effectively with restrictive measures. <b>Note:</b> further detail on how to carry out this assessment is contained within the Guidance Notes.	3. Screen information to: i. verify whether a person, entity or body is designated; ii. manage the risks of violation of restrictive measures; and iii. manage the risks of circumvention of restrictive measures

As always, the EBA notes that Institutions should apply provisions in both Guidelines in a manner that is effective and proportionate to each institution's nature and size, the nature, scope and complexity of its activities, and its exposure to restrictive measures.

These Guidelines will apply from 30th December 2025 and can be accessed on the EBA's Website, linked [here](#).





## EBA Risk Assessment Report

In November 2024, the European Banking Authority (EBA) published its Risk Assessment Report (RAR), highlighting key developments and trends in the EU/EEA banking sector. The report provides an overview of the EBA's outlook on the main risks and vulnerabilities facing the sector. The RAR is based on both qualitative and quantitative data collected by the EBA.

**ML/TF Risk:** One of the risks identified in the report is in relation to Financial Crime, where it is highlighted that the high number of cases of money laundering (ML) and terrorist financing (TF) involving European banks in recent years has caused substantial reputational damage to the banking system and undermines the integrity of the EU/EEA banking sector. According to the Risk Assessment Questionnaire (RAQ) responses, 13% of banks recognize ML/TF risk as a main driver of operational risk. Individual Financial Crime risks highlighted include:

- the implementation of restrictive measures in connection with the Russian war of aggression against Ukraine;
- Customers' transactions received from, or sent to, jurisdictions that are subject to international sanctions; and
- The laundering of proceeds of frauds.

The EBA has continued to address ML/TF related risks through regulation, including two sets of guidelines on internal policies, procedures and controls to ensure the implementation of EU and national restrictive measures, and guidelines on the 'travel rule', i.e. information accompanying transfers of crypto assets and funds.

**EuReCA Reporting:** Between January 1 and August 31, 2024, 32 national competent authorities reported over 600 serious deficiencies, or 'material weaknesses' to EuReCA, the EU's central database for AML/CFT. As has been the trend to date, most reports concerned credit institutions, alongside payment institutions. This was followed by an increase in deficiencies detected in e-money institutions, compared to the previous report. Most deficiencies reported in this period were still related to institutions' approaches to customer due diligence (CDD) practices.

**Fraud Risk:** Fraud risk has also grown significantly in the last 2 years and is considered nearly as relevant as conduct and legal risks. The report notes that risks related to financial crime, but also further digitalisation and technical innovation, including growing usage of AI in financial crime, may have contributed to a continuously growing risk of fraud. RAQ responses point to payment fraud and fraud by theft or breach of customer credentials, including social engineering, as the main drivers of fraud risk (59% agreement), followed by online and cyber fraudulent activities (52% agreement).

You can read the full Risk Assessment Report [here](#).





## EBA Report on the functioning of AML/CFT colleges in 2023

On December 16th 2024, the EBA published its fourth Report on the functioning of anti-money laundering and countering the financing of terrorism (AML/CFT) colleges in 2023. AML/CFT colleges are permanent structures that bring together different supervisory authorities responsible for the AML/CFT supervision of a cross-border financial institution, which operates in at least three Member States. Their aim is to ensure that supervisors exchange information in a timely manner, and that they cooperate to achieve better and more targeted supervisory outcomes in the fight against financial crime. The Report finds that competent authorities (CAs) continued to improve the functioning of AML/CFT colleges in 2023. Nevertheless, further progress is needed especially in two key areas:

- Adjusting the functioning of AML/CFT colleges to the money laundering and terrorist financing (ML/TF) risks to which the underlying firm is exposed, and
- Discussing the need for a common approach or joint action.

The Report sets out findings and observations from EBA staff's monitoring of AML/CFT colleges in 2023, which suggest that, overall, CAs continued to improve the effectiveness of AML/CFT colleges. The EBA, nevertheless, identified two key areas in which the progress made by CAs was seen as insufficient, namely:

- Implementing the risk-based approach to the organisation of colleges - the functioning of colleges was not sufficiently adapted to the risks to which the firms were exposed and to their specificities. This meant that CAs could not allocate their resources in a sufficiently strategic manner.
- Ensuring that discussions on the need for a common approach are meaningful and systematic - one of the main purposes of AML/CFT colleges is to allow CAs to identify common ML/TF risks and AML/CFT issues, and to coordinate the actions they take to address those risks and issues. The EBA found that few colleges had meaningful discussions on these aspects. As a result, CAs were rarely able to identify whether there were risks and/or issues that should be addressed in a coordinated manner.

Addressing the issues mentioned in the two points above will be key to ensuring that AML/CFT colleges can be used by competent authorities to their full potential. The EBA therefore encourages NCAs to prioritise taking steps to improve the functioning of colleges in these areas. Two key recommendations were made in relation to further improving the functioning of AML/CFT colleges in the future:

- Making the organisation of AML/CFT colleges more in line with the risks and specificities of the group; and
- Enhancing discussions on common issues and common approach.

In addition to this, it is noted in the EBA's report that through its thematic monitoring of colleges, the EBA identified ML/TF risks and issues affecting firms of the banking, payment and e-money sectors with a FinTech-oriented business model, that supervisors are invited to better take into consideration.

You can read the full report [here](#).



## EBA Report on NCA's approaches to the supervision of Banks with respect to AML/CFT

In December 2024, the EBA published a report which summarises the EBA's findings from the fourth round of ongoing reviews of national competent authorities' (NCAs') approaches to AML/CFT supervision of banks in the EU/ EEA Member States ('MS'). Over the course of 2023-2024, the EBA's assessed 14 NCAs from 9 MS and issued recommended actions tailored to each NCA to support its AML/CFT work.

The EBA also assessed how prudential supervisors in these member states tackled ML/TF risk in line with their supervisory remit and scope. With the conclusion of this round, the EBA has assessed all 40 NCAs that are responsible for the AML/CFT supervision in 30 EU/EEA MS.

The report found that all NCAs in this round had taken important steps to implement a risk-based approach to AML/CFT and, since the first round of reviews in 2018, has seen significant developments in the NCAs' approaches to supervision. These steps included an enhanced focus on, and investment in, NCAs' risk assessment methodologies and tools, and a marked increase in cooperation, for example in the AML/CFT colleges context. The report notes that most NCAs had restructured their AML/CFT supervisory organisation by creating a stand-alone AML/CFT unit and increasing resources allocated to AML/CFT supervision.

Nevertheless, the review team continued to find areas for improvement, including:

- Weaknesses in the entity-level or sectoral risk assessment methodologies,
- AML/CFT supervision to be lacking a strategic approach,
- The enforcement process not to be fully effective or deterrent,
- Limited cooperation in the absence of AML/CFT colleges,
- Divergent approaches in the way prudential supervisors consider ML/TF risks.

Overall, while the EBA continued to identify issues and shortcomings in the fourth round of reviews, progress made since round one suggests that, by NCAs taking the recommended actions, the effectiveness of AML/CFT supervision in MS will further improve and facilitate the effective implementation of the new AML/CFT package

You can read the full report [here](#).







## EC Report on High Risk areas of corruption in the EU

On November 4th 2024, the European Commission published a detailed report on High-Risk areas of corruption in the EU. This report identified six sectors subject to high corruption risks, namely:

- |                                    |                         |                     |
|------------------------------------|-------------------------|---------------------|
| 1. Public Procurement,             | 3. Healthcare           | 5. Financial Sector |
| 2. Construction and Infrastructure | 4. Defence and Security | 6. Sports           |

Within the report, an in-depth analysis is provided on each of the sectors, which focuses on character, causes and consequences of corruption. In relation to the Financial Sector, it is noted that many types of serious crimes are categorised as corruption, including money laundering, tax evasion, hidden assets, consumer fraud, terrorism financing and cybercrimes. The report highlights a recent EU Proposal on combatting corruption which acknowledges that corruption and money laundering are intrinsically linked, noting that “It is very likely that many financial crimes could not be envisioned, much less successfully carried out, if offenders did not have methods to hide, move, re-label and surreptitiously retain access their illicit gains”.

In relation to the supervision of organisations within the sector, Transparency International notes that Member States have divergent supervisory practices that in many cases have been “ineffective in detecting malpractice by banks in a timely manner and resulting in sanctions.” It said the European Central Bank’s supervision of banks’ AML activities is “very limited” because many issues are handled by national authorities. Transparency International EU notes several shortcomings in regulation and enforcement, including:

- corporate and asset ownership information, and financial data often is unavailable, inadequate, fragmented or of poor quality;
- not all authorities have direct, unfiltered access to information necessary to detect, investigate and prosecute cross-border corruption, including information from non-EU countries;
- authorities may lack tools and technical expertise to crosscheck, process and use the information;
- law enforcement authorities and financial intelligence units often are underfunded and understaffed; and
- coordination among authorities within and outside the EU needs to be improved.

In concluding their review of the Financial Sector, the report provides further areas of consideration and actions that are being taken within the sector to deal with Corruption.

The full report can be found [here](#).





## EBA Report on Tokenised Deposits



On December 12th 2024, the EBA published a report on Tokenised Deposits. The aim of this report is to facilitate awareness of tokenised deposits, as well as assess their potential benefits and challenges. The Report also aims to promote convergence in the classification of tokenised deposits in contrast with electronic money tokens (EMTs) issued by credit institutions under the Markets in Crypto-Assets Regulation (MiCAR). In relation to AML/CFT, the report notes both potential benefits and challenges, including:

### Potential Benefits:

- To some extent, reliance on distributed ledger technology (DLT) for tokenised deposits may facilitate compliance by the credit institution with relevant AML/CFT requirements, compared to deposits recorded on traditional ledgers;
- The use of DLT can significantly enhance transparency and information sharing, albeit the data may need to be coupled with other data in order to be useful for AML/CFT/wider compliance purposes; and
- At present, traditional payment systems might often rely on periodic manual reviews and delayed transaction processing. Real-time capabilities embedded into DLT-based systems for tokenised deposits could enhance the speed and effectiveness of AML/CFT measures, provided that the credit institution has advanced monitoring systems and adequate capabilities to react and process information in a timely manner.

### Potential Challenges:

- Credit institutions may require additional guidance as regards expectations toward the implementation of AML/CFT controls for DLT-based transactions initiated on-chain from tokenised deposit accounts;
- In compiling this report, some competent authorities indicated that credit institutions may benefit from clarity as to whether such transactions would entail a movement of 'funds' or 'crypto-assets' for the purpose of AML/CFT.

The full report can be accessed [here](#).



## Preventing ML/TF in the EU's Crypto Assets Sector

In December 2024, the EBA released a fact sheet covering the prevention of money laundering and terrorism financing in the EU's Crypto Assets Sector. The EBA highlights that the underlying blockchain technology used, when paired with robust compliance, can assist crypto asset businesses and authorities in identifying illicit activities, including ML/TF. However, they note that crypto-assets businesses can be abused for ML/TF purposes. There are some features that make crypto-assets and crypto-assets businesses particularly vulnerable. For instance:

- Crypto-assets have features that hide the identity of customers and make it easier for criminals to conceal their tracks;
- Certain distribution channels and business models are new and neither regulated nor supervised; and
- Some crypto services have a global reach

The fact sheet provides an overview of how the European regulatory approach to tackling ML/TF risk in this sector has evolved since 2013 and confirms that the EU framework, which applies from the end of 2024, introduces four key AML/CFT rules for Crypto Asset Service Providers (CASPs):

1. CASPs, issuers of asset-referenced tokens (ARTs), and issuers of e-money tokens (EMTs) have to seek authorisation to operate in the EU;
2. After obtaining that authorisation, all CASPs and issuers of EMTs have to ensure compliance with EU AML/CFT rules;
3. Issuers of ARTs that are not CASPs or other obliged entities are not 'subject to specific AML/CFT systems and controls rules but still have to ensure that the issuer or the sector are not exposed to serious ML/TF risks and that financial crime is not occasioned, facilitated; and
4. CASPs are required to include specific information on the originator and beneficiary with transfers of crypto-assets to make these transfers traceable. CASPs also have to apply specific measures in relation to transfers of crypto-assets involving self-hosted addresses.

It is noted that entities that CASPs that provided their services in accordance with applicable law before 30 December 2024, may continue to do so until 1 July 2026 or until they are granted or refused an authorisation pursuant to Article 63, whichever is sooner.

The EBA has also outlined in the fact sheet what they are doing to tackle ML/TF risks in the sector, including reviewing Compliance requirements, Market Entry rules and Supervision requirements.

The full fact sheet can be found [here](#).







## EBA criteria to appoint a CCP for CASPs

On December 4th 2024, the European Banking Authority (EBA) launched a public consultation on draft Regulatory Technical Standards (RTS) specifying the criteria according to which crypto-asset service providers (CASPs) should appoint a central contact point (CCP) to ensure compliance with local AML/CFT obligations of the host Member State (MS).

CASPs can provide services in other MS through establishments other than branches. Once established, CASPs have to comply with local AML/CFT obligations, even if their establishments are not 'obliged entities' themselves. This can make the AML/CFT supervision of services provided through these establishments difficult.

To address this, the draft RTS sets out the criteria for determining the circumstances in which the appointment of a CCP is appropriate, as well as the functions of those CCPs. Since the same considerations apply to electronic money issuers (EMI) and payment service providers (PSPs) as they do to CASPs, the EBA proposes to retain the structure and approach set out in Commission Delegated Regulation (EU) 2018/1108 and extend existing provisions to CASPs (leaving the provisions that apply to EMIs and PSPs unchanged), while also introducing new provisions for CASPs where this is necessary in light of their business model and operation.

### Next steps

The draft RTS are published for a two-month public consultation. The EBA will finalise the draft RTS once the consultation responses have been assessed. The final report on draft RTS is envisaged to be published in Q2, 2025.

This consultation runs until 4 February 2025.

You can read more on the consultation [here](#).



# UK Financial Crime Updates





## FCA Financial Crime Guide Updates

On November 29th 2024, the FCA published their revised Financial Crime Guide which includes changes made following their consultation on updates to the Financial Crime Guide earlier in 2024.

The FCA notes that they consulted on proposed changes to the Guide relating to:

- sanctions;
- proliferation financing; and
- transaction monitoring

The FCA also proposed adding references to crypto-assets and the Consumer Duty, along with consequential changes such as data security and updating case studies.

The updated Financial Crime Guide can be accessed [here](#).







## Speech by Emily Shepperd, FCA chief operating officer on Setting the foundations for the FCA's future strategy



On 26 November 2024, Emily Shepperd, FCA Chief Operating Officer (COO), spoke at TheCityUK national conference on the topic of “Setting the FCA foundations for our future strategy”.

Ms Shepard noted that there are four key themes within the FCA's new five year strategy, one of which is “Tackling financial crime”. This focus on financial crime includes fraud and money laundering which Ms Shepard highlighted does enormous damage. It harms consumers and businesses, and undermines trust in the financial system.

Some of the key focus areas for financial crime within the strategy includes:

- Reinforcing partnership working, while also looking internationally to achieve a further step change on the prevalence of financial crime;
- Seeking partnerships to share data where the FCA can, to use data analytics to find connections that help to identify and prosecute the underbelly that operates in financial services;
- Assessing concerns about the cost of financial crime controls and whether there is something that the FCA can do here, while ensuring that the high standards that the UK is known for are not eroded; and
- If organisations are able to confirm identities in a new way, such as through the use of digital passports, can the FCA reduce the need for some of the KYC AML checks that need to be completed when a new customer is being set up.

Ms Shepard notes that the FCA is open to ideas on how they can tackle financial crime more efficiently and proportionately, while maintaining the standards necessary to protect consumers and ensure trust in the system.

You can read the full speech [here](#).

# FATF Financial Crime Updates





## Outcomes FATF Plenary October 2024

In October 2024, 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 Algeria, Angola, Côte d'Ivoire and Lebanon to the list of jurisdictions subject to increased monitoring.
- Jurisdictions no longer under Increased Monitoring: Senegal 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.
- The last two assessment reports in the FATF's fourth cycle of assessments (Argentina and Oman) were approved;
- Members agreed to release for public consultation proposed revisions to the standards related to FATF's ongoing focus on financial inclusion;
- FATF also approved new guidance on national risk assessments to support countries to understand the illicit finance risks they face;
- The FATF also discussed standard changes related to cross-border payment systems and progressed work to identify the latest terrorist financing and proliferation financing risks.
- FATF also commenced a project to review its processes to ensure that countries do not misuse the FATF requirements to restrict the activities of NPOs.
- Members reported on the value of the horizontal review of DNFBPs technical compliance related to corruption to support necessary reforms. FATF decided to continue discussing follow-up on this issue at its next meeting.

Further information on the above topics and more can be read [here](#)







## FATF Guidance: National Risk Assessment

In November 2024, the Financial Action Task Force (FATF) released guidance to assist countries in conducting a National Risk Assessment (NRA) focused on the assessment of money laundering risks.

The document has been developed considering the experience of a range of countries from across the FATF Global Network in the last decade – more than 90 contributed to this guidance – and is meant to demonstrate good practices that have been used by countries to assist others in tailoring these good practices into their own national context. The FATF guidance document contains three sections:

- **Section 1: NRA Preparation and Set-up** – This section identifies the prerequisites to a successful NRA. It covers key foundational parts of the NRA such as political commitment, an inclusive NRA mechanism, objective setting, and the acquisition of information and data.
- **Section 2: Assessing and Understanding Money Laundering Risks** – This section provides a linear, structured approach for countries to follow in conducting their analysis of threats, vulnerabilities, and risks. There is no set methodology that countries must follow, and a country's NRA process should have regard to its capacity, as well as its unique risk and context.
- **Section 3: Post-NRA Actions** – This section identifies simultaneous practices that a country should undertake after the conclusion of the analytical process. It covers the measures that a country could take to ensure that its ML mitigation measures are commensurate with the risks identified, the communication of the NRA's findings, and refining of the NRA process.

FATF notes that this document will be updated upon completion of the proposed changes to the FATF Standards on AML/CFT and Financial Inclusion.

You can read the full FATF Guidance document [here](#).



## FATF Public Consultation: AML/CFT & Financial Inclusion

In October 2024, the Financial Action Task Force (FATF) published a public consultation in relation to considerations on revising FATF Recommendations in order to better align them with measures to promote financial inclusion. This is part of FATF's programme of work to address the unintended consequences of AML/CFT measures. The revisions focus on Recommendation 1 and its Interpretive Note, with corresponding changes to Recommendations 10 and 15 and related Glossary definitions. These proposed revisions aim to better promote financial inclusion through increased focus on proportionality and simplified measures in the risk-based approach, and to give countries, supervisors, and financial institutions greater confidence and assurance when implementing of simplified measures.

The FATF would particularly welcome views on the following issues:

- FATF is considering the replacement of the term “commensurate” with “proportionate” in Recommendation One;
- FATF is considering amendments to require supervisors to “review and take into account the risk mitigation measures undertaken by financial institutions/DNFBPs”,
- On adoption of simplified measures in lower risk situations, FATF proposes to replace “countries may decide to allow simplified measures” with “countries should allow and encourage simplified measures”.
- On “non-face-to-face customer-identification and transactions” as an example of potentially higher-risk situations, addition of qualification (“unless appropriate risk mitigation measures have been implemented”).

Further information on this consultation can be found [here](#).





## FATF Consultation: AML/CFT and Financial Inclusion – AFME Response

In December 2024, the Association for Financial Markets in Europe (AFME) took the opportunity to comment on the Financial Action Task Force (FATF) consultation on AML/CFT and Financial Inclusion.

They welcomed FATF's intention to better align its Recommendations with measures to promote financial inclusion. They broadly support the suggested changes, however, they noted that certain issues are nuanced and need to be carefully considered. AFME noted that the stated purpose of the proposed changes is to address unintended consequences of AML/CFT measures. As the FATF seeks to make improvements, AFME suggested that care must be taken to limit the potential for other unintended consequences to arise.

AFME noted that they are grateful to the FATF for opening this consultation - they consider that effective governance includes active industry outreach, engagement, and consultation – both before and after changes, as well as periodically. This approach from FATF ensures proportionality and supports the appropriate evolution of requirements and guidance.

General comments from AFME were focused on:

- Identification of targeted population;
- Need to avoid conflation of simplified due diligence with financial inclusion;
- Simplified due diligence as a step toward financial inclusion; additional actions from regulators; and
- Need to discourage jurisdictions exceeding common FATF standards.

Furthermore, AFME supported several proposals from FATF and provided commentary on why they support these proposals. The AFME welcome the opportunity to discuss any point made in this paper with FATF.

You can read the full Response [here](#).



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](mailto:sinead.m.ovenden@pwc.com)



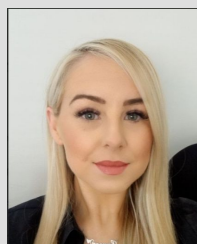
**Aoibheann Morgan**

Director - FS Risk & Regulation  
E: [aoibheann.morgan@pwc.com](mailto:aoibheann.morgan@pwc.com)



**Ri Drozan**

Senior Manager - FS Risk & Regulation  
E: [irina.drozan@pwc.com](mailto:irina.drozan@pwc.com)



**Lauren Cleary**

Manager - FS Risk & Regulation  
E: [lauren.cleary@pwc.com](mailto:lauren.cleary@pwc.com)



© 2025 PwC. The information contained in this newsletter is for general guidance on matters of interest only. The application and impact of laws can vary widely based on the specific facts involved. Given the changing nature of laws, rules and regulations, and the inherent hazards of electronic communication, there may be delays, omissions or inaccuracies in information contained in this newsletter. Accordingly, the information on this newsletter is provided with the understanding that the authors and publishers are not herein engaged in rendering legal, accounting, tax, or other professional advice and services. As such, it should not be used as a substitute for consultation with professional accounting, tax, legal or other competent advisers. Before making any decision or taking any action, you should consult a PwC professional. While we have made every attempt to ensure that the information contained in this newsletter has been obtained from reliable sources, PwC is not responsible for any errors or omissions, or for the results obtained from the use of this information. All information in this newsletter is provided "as is", with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this information, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, merchantability and fitness for a particular purpose. In no event will PwC, its related partnerships or corporations, or the partners, agents or employees thereof be liable to you or anyone else for any decision made or action taken in reliance on the information in this newsletter or for any consequential, special or similar damages, even if advised of the possibility of such damages.

Certain links in this newsletter connect to other websites maintained by third parties over whom PwC has no control. PwC makes no representations as to the accuracy or any other aspect of information contained in other websites.