Q4 2022 Financial Crime Quarterly Update

October - December

Introduction

Welcome to the latest edition of our Quarterly Financial Crime newsletter, which outlines all of the latest news and regulatory updates across the world of Financial Crime.

In Ireland, there have been updates in relation to access to the RBO, as well as updated information in relation to Ireland's Safe Deposit Box Bank and Payment Accounts Register (ISBAR). The IMF also published their Financial Sector Assessment Program-Technical Report on Anti-Money Laundering / Combating the Financing of Terrorism for Ireland.

From a European perspective, in November 2022, the European Banking Authority (EBA) published its final Guidelines on the use of remote customer onboarding solutions and the European Payments Council also published their annual "Payment Threat and Fraud Trends Report".

Globally, the Wolfsberg Group published its updated Financial Crime Principles for Correspondent Banking in October of this year to provide guidance and best practices for banks.

We hope you enjoy reading this newsletter, which contains further details on the issues outlined above, and more! We also would like to wish you a Merry Christmas and a very Happy New Year.

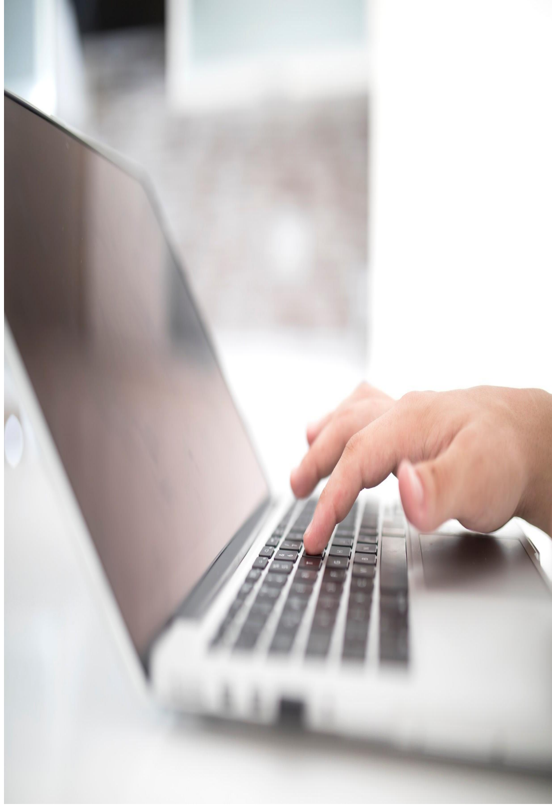
Sinead Ovenden

Partner, FS Risk and Regulation

Contents

1

IRISH FINANCIAL CRIME UPDATES



Access to Beneficial Ownership Register restricted following Court of Justice of the EU ruling

On 22 November 2022, the Court of Justice of the European Union ruled that the provision under the AML Directive whereby the information on the beneficial ownership of companies incorporated within the territory of the Member States is accessible in all cases to any member of the general public is invalid.

This ruling was provided following a series of questions being referred to the court by the Luxembourg District Court. These queries considered the interpretation of certain provisions of the anti-money laundering directive and the validity of those provisions in the light of the Charter of Fundamental Rights of the European Union (‘the Charter’).

The Court ruled that “the general public’s access to information on beneficial ownership constitutes a serious interference with the fundamental rights to respect for private life and to the protection of personal data, enshrined in Articles 7 and 8 of the Charter, respectively. Indeed, the information disclosed enables a potentially unlimited number of persons to find out about the material and financial situation of a beneficial owner. Furthermore, the potential consequences for the data subjects resulting from possible abuse of their personal data are exacerbated by the fact that, once this data has been made available to the general public, they can not only be freely consulted, but also retained and disseminated.

In light of this, the Central Register of Beneficial Ownership of Companies and Industrial and Provident Societies (RBO) in Ireland, has restricted access to search the register to Designated Persons and Competent Authorities only, with very limited information being available to other parties in accordance with the recent ruling of the Court of Justice of the European Union.

Ireland Safe Deposit Box Bank and Payment Accounts Register (ISBAR)

In February 2022, under the European Union (Anti-Money Laundering: Central Mechanism for Information on Safe-Deposit Boxes and Bank and Payments Accounts), the Department of Finance conferred responsibility for the establishment of Ireland Safe Deposit Box Bank and Payment Accounts Register (ISBAR), on the Central Bank of Ireland ("CBI").

Following this, in October 2022, the CBI launched a web page with more details on how ISBAR will operate. Among the documents added to that webpage are Guidelines on Scope and Reporting, FAQs, and technical guidance documents.

The register identifies the holders and beneficial owners of bank and payment accounts and safe-deposit boxes in Ireland. The purpose of this is to help establish links between suspicious transactions and underlying criminal activity. The register ensures that flows of money can be properly traced to individuals, entities and illicit networks at an early stage.

Note: All credit Institutions established in Ireland are required to report to ISBAR, if:
- Irish IBANS are issued; or
- Safe Deposit Boxes are held.

Two separate returns will be made available to credit institutions for the purpose of ISBAR reporting; one for bank and payment accounts, and one for safe deposit box information. Credit institutions who do not offer a safe deposit box service, must complete an attestation form to confirm where this return is not applicable.

Link to the webpage can be accessed here:
https://www.centralbank.ie/regulation/anti-money-laundering-and-countering-the-financing-of-terrorism/ireland-safe-deposit-box-bank-and-payment-accounts-register-(isbar)#:~:text=ISBAR%20FAQ-,Ireland%20Safe%20Deposit%20Box%20Bank%20and%20Payment%20Accounts%20Register%20(ISBAR,transactions%20and%20underlying%20criminal%20activity.

Ireland: Financial Sector Assessment Program-Technical Note on Anti-Money Laundering/Combating the Financing of Terrorism

On October 21st 2022, the International Monetary Fund (IMF) published the Financial Sector Assessment Program-Technical Report on Anti-Money Laundering/Combating the Financing of Terrorism for Ireland.

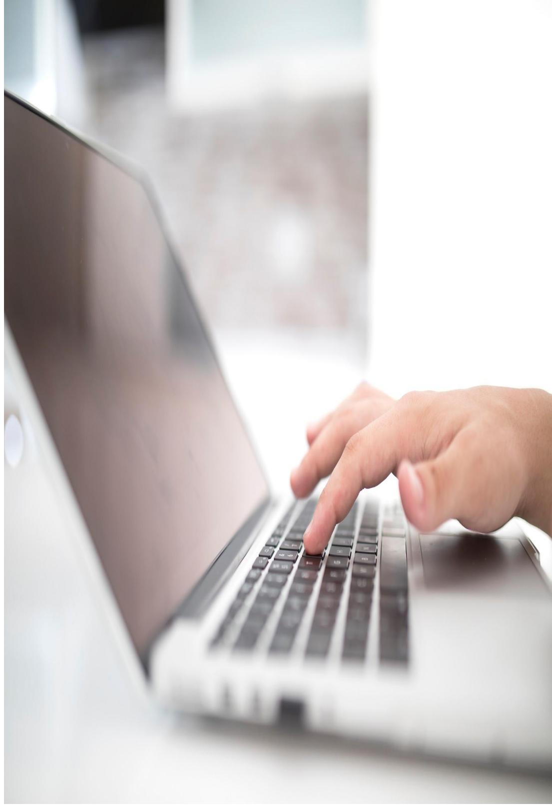
As it is only a Technical report, it does not rate Ireland but simply provides a high level overview. Some of the key highlights from the report are listed below:

- While domestic money laundering threats are well understood by authorities, as a growing international financial center, Ireland is exposed to inherent transnational money laundering and terrorist financing (ML/TF) related risks. The ML risks facing Ireland include illicit proceeds from foreign crimes (e.g., corruption, tax crimes).
- Retail and international banks, trust and company service providers (TCSPs), lawyers, and accountants are rated as medium to high-risk for ML, while virtual asset service providers (VASPs) pose emerging risks.
- As for Brexit, the recent move of international banks to Dublin, and the COVID-19 pandemic increased the money laundering risks faced by Ireland. The Central Bank of Ireland nevertheless has demonstrated a deep and robust experience in assessing and understanding their domestic ML/TF risks. However, the IMF notes that an increased focus on risks related to transnational illicit financial flows is required.
- A thematic risk assessment undertaken by the Anti-Money Laundering Steering Committee (AMLSC) of international ML/TF risks would enhance the authorities’ risk understanding and is key to an effective response to the rapid financial sector growth.
- Introducing data analytics tools, including machine learning to leverage potentially available big data on cross-border payments, would allow for efficient detection of emerging risks. The results of this assessment should be published to improve the understanding of transnational ML/TF risks and fed into the anti-money laundering and combating the financing of terrorism (AML/CFT) policy priorities going forward.

The full report is available here:
https://www.imf.org/en/Publications/CR/Issues/2022/10/20/Ireland-Financial-Sector-Assessment-Program-Technical-Note-on-Anti-Money-Laundering-524936

2

EUROPEAN FINANCIAL CRIME UPDATES



EBA publishes guidelines on remote customer onboarding

On November 22nd, the European Banking Authority (EBA) published its final Guidelines on the use of remote customer onboarding solutions.

- These new guidelines complement existing guidelines with specific instructions on the steps credit and financial institutions should take when choosing remote customer onboarding tools, and when ascertaining whether these tools are sufficient to enable them to comply effectively with their initial CDD obligations.
- The guidelines establish common EU standards on the development and implementation of sound, risk-sensitive initial customer due diligence policies and processes in the remote customer onboarding context.
- They set out the steps financial institutions should take when choosing remote customer onboarding tools and when assessing the adequacy and reliability of such tools, in order to comply effectively with their AML/CFT obligations. The Guidelines are technologically neutral and do not prioritise the use of one tool over another.
- In relation to Governance, it is noted in the guidelines that the AML/CFT Compliance Officer, should as part of their general duty to prepare policies and procedures to comply with the CDD requirements, make sure that remote customer onboarding policies and procedures are implemented effectively, reviewed regularly and amended where necessary.
- The guidelines outline that a pre-implementation assessment of the remote customer onboarding solution should be carried out when considering whether to adopt a new solution.
- Ongoing monitoring of the remote customer onboarding solution should be implemented to ensure that the solution operates in line with expectations.
- It remains the responsibility of the Credit and Financial institutions to set out in their policies and procedures the information needed to identify the customer, the types of documents, data, or information the institution will use to verify the customer’s identity and the manner in which this information will be verified.
- Remote customer onboarding solutions implemented by a credit and financial institutions should, as a minimum, allow for the following, as part of their verification process:
    a. a) there is a match between the visible information of the natural person and the documentation provided;
    b. b) where the customer is a legal entity, it is publicly registered, where applicable;
    c. c) where the customer is a legal entity, the natural person that represents it is entitled to act on its behalf.

The deadline for competent authorities to report whether they comply with the guidelines will be two months after the publication of the translations.

The full set of Guidelines is available here:
https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2022/EBA-GL-2022-15%20GL%20on%20remote%20customer%20onboarding/1043884/Guidelines%20on%20the%20use%20of%20Remote%20Customer%20Onboarding%20Solutions.pdf

EBA consultation on the effective management of ML/TF risks when providing access to financial services

On December 6th 2022, the European Banking Authority ("EBA") launched a public consultation on new Guidelines on the effective management of ML/TF risks when providing access to financial services. The consultation aims to ensure that customers, especially the most vulnerable ones, are not denied access to financial services without valid reason. This consultation runs until 6 February 2023.

The EBA note that access to at least basic financial products and services is a prerequisite for organisations and individuals to participate in modern economic and social life. It can also save the lives of vulnerable customers, such as refugees or homeless people. However, such access is not always ensured.

01 EBA ML/TF Risk Factor Guidelines Amendment

This consultation is in relation to adding a new section to the EBA's ML/TF risk factors Guidelines, which set out what financial institutions should do to identify and tackle ML/TF risk. This new section will help financial institutions understand how Not-for-Profit Organisations are organised, how they can be different from other customers and what they can do to manage ML/TF risks associated with such customers effectively instead of denying them access to financial services.

02 Effective management of ML/TF Risks when providing access to financial services

The second consultation tackles the issue of effective management of ML/TF risks by financial institutions when providing access to financial services. These Guidelines clarify the interaction between the access to financial services and institutions' AML/CFT obligations, including in situations where customers, including the most vulnerable, have legitimate reasons to be unable to provide traditional forms of identity documentation. In addition, they set out the steps institutions should take when considering whether to refuse or terminate a business relationship with a customer based on ML/TF risk or AML/CFT compliance grounds.

The consultation paper can be accessed here:
https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Consultations/2023/Consultation%20on%20effective%20management%20of%20ML-TF%20risks%20when%20providing%20access%20to%20financial%20services%20%28EBA-CP-2022-13%29/1044816/Consultation%20paper%20on%20amending%20risk%20factor%20GLs%20and%20GLs%20on%20access%20to%20financial%20services.pdf

EBA Annual Work Programme for 2023 Published

In September 2022, the European Banking Authority ("EBA") published its annual work programme for 2023, describing the key strategic areas of work for the Authority for the coming year, as well as related activities and tasks.

This included key areas of focus within Financial Crime, including:

1. Digital finance and the delivery of MiCA/DORA mandates
2. Enhancing capacity to fight ML/FT in the EU

1. Digital finance and the delivery of MiCA/DORA mandates

- The EBA work programme notes that both the Markets in Crypto Assets Regulation ("MiCA") and the Digital Operational Resilience Act ("DORA") are expected to enter into force in 2023, while the date of application is anticipated for 1 January 2025. The EBA, together with the other ESAs (where necessary), will need to develop the vast policy work from MiCA and DORA in advance of the application date.
- In 2023, the EBA together with ESMA and EIOPA will be partnering with the European Commission to the activities of EU Supervisory Digital Finance Academy. The Academy will aim to strengthen supervisory capacity in innovative digital finance, thus supporting the objectives of the EU Digital Finance Strategy.
- The EBA will continue to monitor financial innovation and identify areas where further regulatory or supervisory response may be needed.

2. Enhancing capacity to fight ML/FT in the EU

- In 2023, the EBA will continue to lead, coordinate, and monitor the EU financial sector's fight against ML/TF in line with its legal mandate. This will include supporting the implementation of robust approaches to AML/CFT supervision across the EU; contributing to the implementation of a holistic approach to tackling ML/TF, sanctions and other financial crimes; and providing sound, technical advice to stakeholders to promote the effective design and implementation of the EU's new institutional AML/CFT framework
- The EBA will also prepare to hand over those aspects of its work that relate exclusively to AML/CFT compliance and supervision to the new AML/CFT Authority (AMLA). The transfer of powers is currently expected to take place in 2024.

Annual European Payments Council “Payment Threat and Fraud Trends Report”

On December 9 2022, the European Payments Council published their annual Payment Threat and Fraud Trends Report. This report provides an overview of the most important threats and other “fraud enablers” in the payments landscape. Some of the key highlights from this report include:

- Social engineering attacks and phishing attempts are still increasing. Awareness campaigns are still very important countermeasures against social engineering, and these campaigns should be coordinated, involving also public administrations. They should target individual and corporate customers, as well as employees.
- Malware remains a major threat, in particular ransomware has been on the rise during the past year, requiring new mitigating measures.
- One of the most sophisticated and lucrative types of payment fraud now and for the future seems to be Advanced Persistent Threat (APT). It must be considered as a potential high risk not only for payment infrastructures but also for all network related payment ecosystems.
- A fraudulent payment transaction is often followed by the use of a monetisation channel such as an immediate cash withdrawal, a purchase with no trace, a money transfer or a transfer to another account (“money mulling”).

The report notes that an important aspect to mitigate the risks and reduce fraud is the sharing of fraud intelligence and information on incidents amongst Payment Service Providers.

The full report can be accessed here:
https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2022-12/EPC183-22%20v1.0%202022%20Payments%20Threats%20and%20Fraud%20Trends%20Report.pdf

European Court of Auditors high-level seminar, 'New EU AML-CTF supervision model: expectations vs feasibility'

In September 2022, Ms Mairead McGuinness, Commissioner for financial services, financial stability and Capital Markets Union, opened the European Court of Auditors (ECA) high level seminar on anti-money laundering (AML) : “New EU AML/CTF supervision model: expectations vs feasibility”. In her speech, the Commissioner *reiterated the importance of AML Regulation:*

“Maybe to say that sometimes when we talk about rules and regulations around money laundering, and indeed around other topics, they sound dry. It's about rules, and procedures, and all that goes with that. But fundamentally, when we talk about money laundering, we're talking about trust and integrity – or indeed the attack on trust and integrity in our financial system. As citizens, we should be able to trust the financial system. Dirty money destroys trust and corrupts the system. We cannot allow dirty money to be laundered and cleansed of its illegal and corrupt origins through our financial institutions.”

Commissioner McGuiness spoke about four different elements, which together represent a new European approach to fight money laundering and the financing of terrorism:

1. The new AML Regulation
2. The new AML Directive
3. The extension of the Transfer of Funds Regulation to the virtual and crypto space
4. The new EU Anti-Money Laundering Authority ("AMLA").

In particular, Commissioner McGuiness noted that the introduction of the AMLA is a game-changer in the fight against money laundering. The AMLA is set to become the center of our new supervisory system, undertaking some supervision itself, all while fostering convergence and a common culture among national supervisors.

The full speech is available here: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_22_5593

Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities

On 27 October 2022, the European Commission adopted its third supranational risk assessment report (SNRA), a tool to help Member States identify and address money laundering and terrorist financing risks.

The report analyses the present ML/TF risks and proposes a comprehensive action plan to address them. It also examines the degree to which previous recommendations for mitigating measures in the 2019 report have been implemented and evaluates the remaining risks. It also benefits from the work and stakeholder consultation process that led to the adoption of the Commission's Action Plan of 2020 and the legislative AML/CFT package proposed in 2021.

The report shows that while most recommendations of the previous assessments (the last such report dates from 2019) have already been implemented, it underlines the fact that weaknesses in identifying beneficial ownership continue to remain a considerable threat to the financial system, as anonymity remains a critical vulnerability for all sectors and activities.

The report also re-calculates the risk levels of certain areas where changes have been detected since 2019, e.g. crypto-assets and online gambling, where risks are now higher.

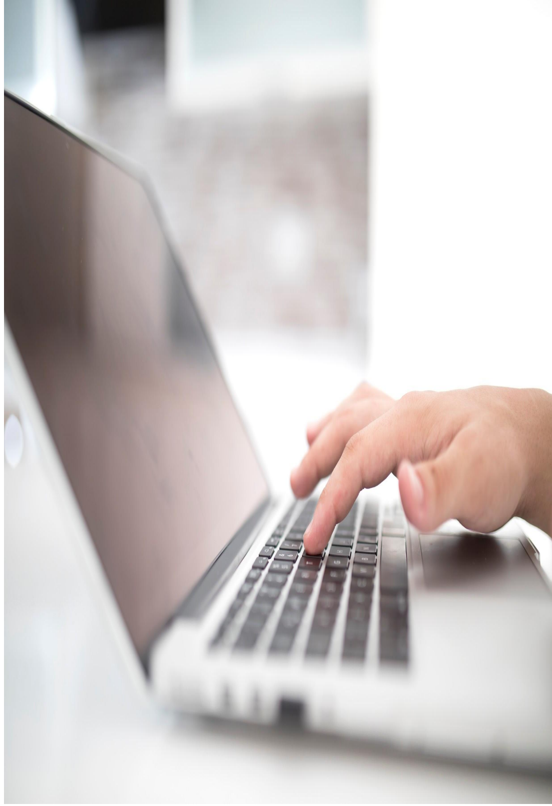
The SNRA sets out mitigating measures that the EU and national governments should take to address the risks identified. It makes several recommendations, particularly that:

- Member States should fully implement the provisions set out in the Anti-Money Laundering Directive (AMLD) about beneficial ownership registers.
- Member States should ensure that their national risk assessments cover the risks associated with financial products and services, and provide appropriate mitigating measures.
- Member States should demonstrate that anti-money laundering (AML) supervisors can fully carry out their tasks.
- Encourage close cooperation between AML competent authorities, financial intelligence units (FIUs), law enforcement authorities and the private sector.

The Commission remains committed to protecting EU citizens and the financial system from money laundering and terrorist financing. The recent anti-money rules (AML) rules proposed in the 2021 legislative package, aim at improving the detection of suspicious transactions and activities, and close loopholes used by criminals to launder illicit proceeds or finance terrorist activities through the financial system. The SNRA recognises the importance of this package, which is currently being discussed by the European Parliament and the Council.

The full report is available here:
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022SC0344&from=EN

3 GLOBAL FINANCIAL CRIME UPDATES



Publication of the Wolfsberg FC Principles for Correspondent Banking

On October 28, 2022, the Wolfsberg Group published its updated Financial Crime Principles for Correspondent Banking. This document updates the 2014 version and provides guidance and best practices for banks, draws a distinction between Correspondent Relationships and Correspondent Banking activity, addresses entities other than banks who have Correspondent Relationships, and incorporates revised Frequently Asked Questions that were previously a separate document.The updated principles promote effective risk management and enable Financial Institutions (FI) to exercise sound business judgment regarding their correspondent banking customers. Throughout the report, the Wolfsberg Group advocates that FIs adopt a risk-based approach to each principle – allocating their resources and level of response according to the level of risk presented.

Applicable to all correspondent banking relationships that an FI establishes or maintains for a respondent, the Wolfsberg Group principles include:

- Defining policies and procedures that require specified personnel to be responsible for ensuring compliance with all correspondent banking activity (Note: All responsible personnel must have relevant experience and have undergone training on the risks involved in Correspondent Banking);
- Identifying and defining an acceptable risk appetite that has been approved by the Board or other similar senior stakeholders
- Undertaking appropriate due diligence, assessing factors such as geographic location, ownership and management structures, and the quality of the respondent's financial crime controls (FCC) program (Note: the principles outline that FI should not rely solely on the fact that a Respondent operates in, or is subjected to, a regulatory environment which is recognised internationally as adequate in the fight against financial crime - this must be assessed in conjunction with other information)
- Applying enhanced due diligence (EDD) to respondents that pose more significant risks, such as politically exposed persons (PEPs) or Downstream FIs
- Implementing policies and procedures to detect, investigate, and report unusual or suspicious activity, including guidance on what is considered to be suspicious;
- Reviewing respondent relationships on an ongoing basis to ensure that the relationship remains within risk appetite.

The full set of principles can be found here:
https://www.wolfsberg-principles.com/sites/default/files/wb/Wolfsberg%20Correspondent%20Banking%20Principles%202022.pdf

Basel AML Index 2022: 11th Public Edition

In early October 2022, the Basel Institute on Governance published the 11th Basel AML Index for the year of 2022 which provides an independent annual ranking of the risks of ML/TF in jurisdictions around the world, on a country-by-country basis. The ML/TF risk is defined as a jurisdiction's vulnerability to ML / TF and its capacities to counter it; it is not intended as a measure of the actual amount of ML/ TF activity in a given jurisdiction.The report is based on a composite methodology with number of indicators categorized into the five key factors considered to contribute to a high money laundering/terrorist financing risk:

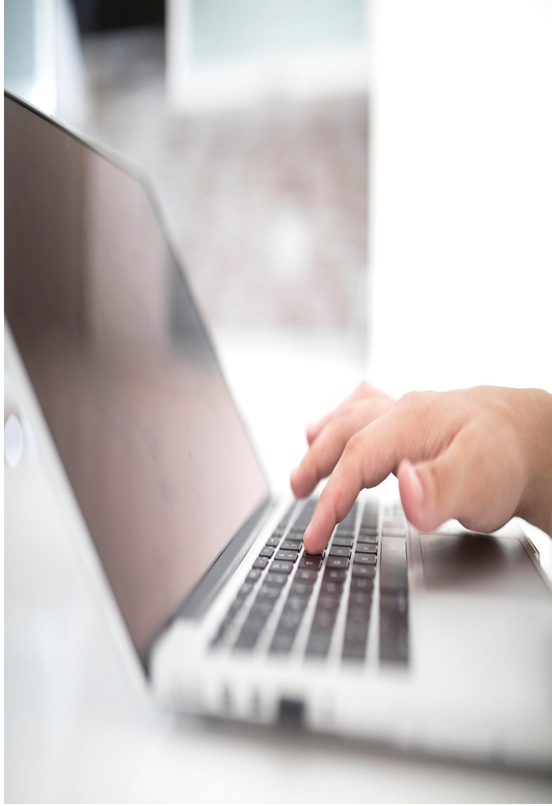
1. Quality of AML / CFT Framework,
2. Risk of Corruption,
3. Financial Transparency and Standards,
4. Public Transparency and Accountability,
5. Legal and Political Risk

Some of the key highlights from the Basel AML Index 2022 report are listed below:

- In the fight against financial crimes, most countries stayed behind criminals seeking to launder illegal funds. The average global money laundering risk according to this year's Index is stuck at 5.25 out of 10, where 10 is the maximum risk level. A tiny decrease in risks relating to the quality of AML/CFT frameworks has been offset by increased risks in the other four areas measured by the Basel AML Index: corruption, financial transparency, public transparency, and political/legal risks.
- Governments, as well as financial institutions and other reporting agencies, are generally getting better at assessing money laundering risks and applying a risk-based approach to addressing them, while risks persist in areas where criminals act fast and innovate (e.g: crypto assets),
- Authorities are progressing very slowly in areas that have long been a weak spot for money laundering/terrorism financing, such as ultimate beneficiary transparency and international cooperation.
- Even where technical compliance with standards improves, effectiveness indicators often drop. In key weak spots such as beneficial ownership transparency and the quality of financial supervision, the gap is growing between technical compliance with the Recommendations of the Financial Action Task Force (FATF) and assessments of the effectiveness of measures in practice

The full report is available here: https://index.baselgovernance.org/api/uploads/221004_Basel_AML_Index_2022_72cc668efb.pdf

4 FATF INSIGHTS



FATF Plenary, 20-21 October 2022 - Outcomes

The first Financial Action Task Force (FATF) plenary under the Presidency of T. Raja Kumar of Singapore took place in Paris in October, 2022.

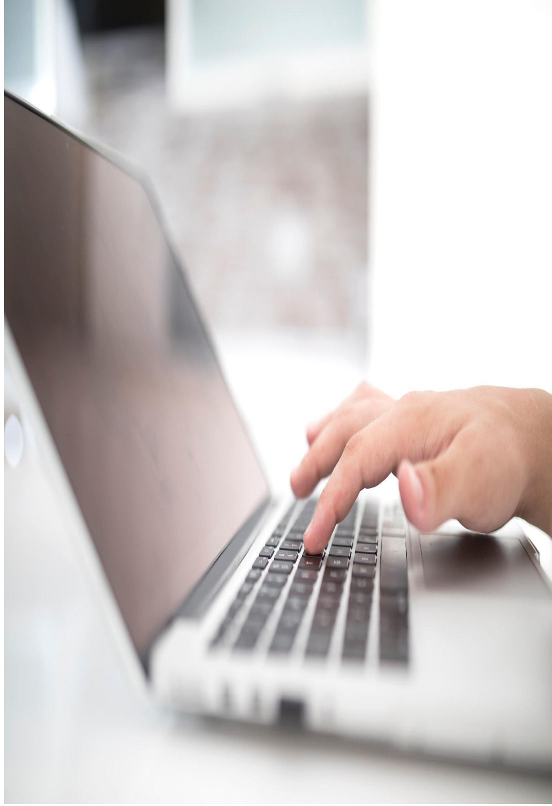
The FATF plenary included discussions on:

- Changes to jurisdictions under increased monitoring
- Further restrictions placed on Russia's FATF membership
- Improving asset recovery
- Strengthening requirements on beneficial ownership
- Undertaking new projects to enhance global anti-corruption efforts
- Providing guidance on detecting and disrupting illegal fentanyl trafficking

Points to number from this Plenary include the following:

- Myanmar is subject to a call for action, having been identified as having serious strategic deficiencies to counter money laundering, terrorist financing, and financing of proliferation.
- New jurisdictions subject to increased monitoring are the Democratic Republic of Congo (DRC), Mozambique and Tanzania.
- Nicaragua and Pakistan are no longer subject to the FATF's increased monitoring process and have been removed from the Grey List.
- Russia is barred participating in meetings of the FATF-Style Regional Bodies as an FATF Member. as it continues to violate FATF core principles which aim to promote security, safety and integrity of the financial system.
- Participants agreed on the importance of a strong legal framework to effectively pursue asset recovery, that action is needed to ensure that international cooperation occurs more rapidly and smoothly, and that the FATF's Standards need strengthening so that countries are better equipped to act effectively at every stage of the asset recovery process.
- To guide countries and the private sector in implementing new requirements under Recommendation 24, the FATF has developed Guidance on Beneficial Ownership which will be released for full public consultation to solicit wider input from stakeholders. The FATF expects to finalise the guidance in February 2023.
- The Plenary also addressed the upcoming report (released November 2022) on illicit proceeds generated from the fentanyl and related synthetic opioids supply chains. The report includes risk indicators that can help identify suspicious activity and makes recommendations on the best approaches to detect and disrupt financial flows relating to this illegal trade.

5 How PwC can help you



PwC Financial Services Regulatory Team

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 completing an 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

Customer Due Diligence & ESG

Our team are experienced in designing policies and procedures for conducting ESG risk assessments, as well as identifying ESG risk:

- Leveraging our established due diligence and risk assessment process to support firms in identifying ESG risk in their customer portfolios and creating a suitable ESG framework.
- Providing access to our network of ESG practitioners consisting of Subject Matter Experts, trainers, experienced project managers and due diligence analysts.

AML Remediation Programmes

PWC is an expert 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 client outreach and independent quality assurance.

AML Risk Mitigation

Adequate risk assessment is at the core of management of AML/TF and is a key area of focus for the CBI. We can support you to identify and assess AML risk through:

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

Target Operating Model

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

- Reviewing your current FC 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

Contacts

FS Risk and Regulation - Financial Crime

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

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

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

Karolina Zugaj
Manager - FS Risk & Regulation
E: karolina.zugaj@pwc.com