Challenges raised by the set-up of the AMLA

1. Key priorities and objectives of AMLA

The Chair highlighted that anti-money laundering (AML) and countering the financing of terrorism (CFT) remain high priorities for the public and private sectors. The associated risks continue to grow, and at the same time there are new regulations and the establishment of the new Anti-Money Laundering Authority (AMLA). The panel will consider institutional, regulatory, and technical hurdles in implementing AMLA, as well as practical methods for utilising and securing technological solutions.

2. Institutional and supervisory challenges for AMLA

The Chair noted that one of AMLA's key tasks is to foster a common supervisory culture and achieve convergence across Europe. A regulator highlighted the experience gained from the functioning over the last 14 years of the European Securities and Markets Authority (ESMA), the European Insurance and Occupational Pensions Authority (EIOPA) and the European Banking Authority (EBA). A crucial ingredient for AMLA's goals is a commitment to risk-based supervision, including across all national competent authorities (NCAs), and for those working on AML to employ a consistent methodology. Joint inspections facilitate the implementation of a risk-based methodology and ensure uniform application of rules.

In terms of technology, a central data and intelligence hub with consistent analytical tools is essential. Discussions regarding data usage highlight the need for flexible, expandable databases facilitated by new technology. Credible enforcement power, demonstrated through joint inspections and visible results at the EU level, instils respect for the institutions.

Obstacles exist at the national level, particularly given different levels of development in AML practices. Some countries have well-established risk-based methodologies, while others do not. Convergence here presents a challenge. National traditions regarding AML and supervision, data fragmentation and confidentiality concerns pose difficulties.

A perceived loss of sovereignty by national authorities, when central bodies discuss new supervisory responsibilities is another obstacle. The political sensitivity of AML means there is a need for independent national supervisors to ensure successful oversight.

Mechanisms for improvement include public/private cooperation, such as that seen in the Netherlands and the United Kingdom. Industry should actively contribute. Clear communication of the expectations from supervisors to industry, and vice versa, is also important.

A supervisory authority suggested that a distinction should be made between supervision and regulation. The key to supervision is having a risk-based approach and proportionality. Focus must remain on the real risks, without excessive requirements for lower-risk areas and factoring in different business models. Requirements must reflect the differences between established banking sectors and new FinTechs.

The current simplification exercise by the Commission presents a valuable opportunity that should be seized, as priorities inevitably shift within the EU. There should be consideration of what is necessary, and what might no longer be necessary.

These actions are needed at all levels, including by NCAs and national governments. It is not only for AMLA, other European Supervisory Authorities (ESAs) and the Commission. Level two and level three regulations should be prepared in close cooperation with obliged entities, with the inclusion of industry associations in the process of creating regulatory technical standards (RTSs) and other level two and three instruments. Their views on compliance costs should be factored in. These regulations must also be clear and unambiguous. Q&As are currently largely managed by the Commission, which has limited expertise in this area, so the process of answering questions is very lengthy. It would be beneficial to return Q&As to the ESAs.

Concerning the interaction between AMLA and NCAs, the latter should retain sufficient flexibility due to their proximity to obliged entities and their understanding of national specificities. However, close cooperation with AMLA will remain essential. The institution of binding instructions from AMLA towards NCAs raises legal questions regarding responsibility and at which court it would be possible to make challenges. This interaction may prove complicated, while similar mechanisms in the banking union and Single Supervisory Mechanism (SSM) have not been used.

3. Ensuring supervisory convergence and a common supervisory culture

A regulator emphasised that people are also important. Secondments and rotation between NCAs and European regulators foster a shared supervisory culture. Individuals returning from such placements prove valuable in integrating a common European perspective into daily work. People are a vital ingredient for creating and keeping the supervisory culture unified.

The Chair added that assembling good quality people and establishing collaborative working methods, involving representatives from national authorities, will be crucial for AMLA's ability to achieve convergence and reach a common culture. AMLA is actively implementing this approach through integrating seconded of national experts from the Member States and by structuring its working methods accordingly.

4. Technology and data-sharing in support of AML supervision

The Chair indicated that substantial investments are being made by national supervisors in Supervisory Technology (SupTech) tools designed to enhance their day-to-day work and asked how AMLA and NCAs could best coordinate these investments.

A regulator identified collaboration on data standardisation and joint technology investment as key drivers for the success of AMLA and the new European system. If not approached correctly then it will just be another layer of bureaucracy where data is collected separately. Four interconnected concepts that are crucial to achieving this are governance, standardisation, common investment and feedback loops.

Regarding governance, there should be thinking about predictability, how data standards are set and how data is collected. There should be a collaborative effort between AMLA, NCAs and obliged entities to determine essential data requirements for effective prevention of money laundering and terrorist financing. That demands early strategic development of data standards, even amidst the ongoing efforts to establish the foundational framework for AMLA's operations.

Standardisation and predictability are crucial for reducing inconsistency and duplication in reporting, to avoid having 27 different standards and formats. There has to be clarity about the processes from an early stage when collecting data. The data should be collected in a predefined timeframe, and there should be consideration of interoperability between NCAs, AMLA and the firms, which can be achieved through application programming interfaces (APIs) and by drawing lessons from existing frameworks such as Common Reporting (COREP) and Financial Reporting (FINREP). In addition to being as flexible as possible, there must be mechanisms for recalibration to allow for rapid responses to emerging risks.

In terms of common investments, everyone is developing useful tools, and there is extensive innovation occurring within the private sector and NCAs. These are valuable, but building up a common supervisory culture is about scale. To scale up to the European level, there has to be consideration of how to share, commonly prioritise and co-fund, so that what is effective and efficient can be identified. That does not require a complex framework, but it will need a mechanism through which those key decisions can be made.

Finally, the importance of establishing robust feedback loops involving all stakeholders should be underlined. The private sector knows what automation can do and where it can be helpful, while NCAs and AMLA can indicate what is not useful in practice.

An industry representative outlined a framework encompassing three key areas within the non-bank financial institution landscape. Technology implementation is fundamentally driven by trying to mitigate the specific risks faced by the sector. The primary risk for the non-banking financial sector comes from unbanked customers. One of the reasons regulatory authorities say money transmitting is a high-risk sector, for example, is because it manages numerous unbanked customers dealing in cash.

Technology assists in conducting comprehensive entity and customer risk assessments and potentially putting them on interdiction lists based on pre-defined risk appetite thresholds or identified AML concerns. This encompasses the full spectrum of processes from onboarding controls and know your customer (KYC) procedures, utilising new technologies for identity verification, sophisticated behaviour monitoring techniques, and the collection of transaction-related data and profile changes.

A significant challenge lies in the fact that those actively engaged in financial crime often possess greater technological proficiency and resources than those attempting to counter it, meaning industry efforts often lag. A critical question is whether that slowness is due to regulatory frameworks not adapting quickly enough to address rapidly evolving criminal typologies. For example, overly strict information requirements for unbanked customers requiring data those individuals may legitimately not possess, can inadvertently drive transactions into unregulated and opaque channels, effectively increasing systemic risk rather than mitigating it.

There is increasingly sophisticated use of AI to falsify identities. One report indicated a concerning 40% success rate in such AI-created false IDs bypassing existing monitoring systems, which clearly poses a risk to financial institutions and regulatory authorities.

Regulators and financial institutions must work together to mitigate that risk quickly and effectively, which should mean taking a risk-based approach. That involves conducting risk assessments all the way through to monitoring, consideration of the customer base, and consideration of the countries being operated in. Focusing solely on European contexts ignores critical risks originating from receive markets like Africa and South Asia, for example. There is a need for collaborative, proactive strategies involving global regulators and using technological innovations, to effectively address cross-border financial crime.

5. Balancing effectiveness and compliance costs

An industry representative referred to three major challenges. The first is harmonising without making the situation too complex. There is general agreement about the benefits of harmonisation, having a level playing field and simplification. One of the initial goals of the SSM, which was established in 2014, was to achieve harmonisation. Discussions over the past two days at Eurofi have been heavily focused on the need to simplify, which demonstrates that the SSM harmonisation probably came with excessive complexity. There is an opportunity to try to harmonise in AML, but the over complication seen in the SSM should not be repeated for AML.

Efforts should be made to avoid making AML too complex. One aspect of that is favouring a principles-based approach that relies mostly on level one texts, to avoid the gold plating tendency that stems from levels two and three. Perfection should not be the goal.

Additional EU layering onto already complex national regulations should be limited, as such additions will make the situation very complex for banks. Adding something centrally implies a need to reduce the burden at the local level.

A third aspect is having a proportionate risk-based approach and accommodating diverse business models by being proportionate relative to the risks. That is particularly important given AML regulation extends beyond banking to encompass numerous actors across various sectors.

A key success factor for supervision is trust between supervisors and industry participants. Relying slightly more on trust and slightly less on rules is an effective way to proceed. Trust is achieved through efficient supervisory dialogue, which includes supervisors actively listening to banks.

Banks, especially retail banks in the EU, have a strong incentive to comply with regulations as doing so helps preserve their reputations. The issue of reputational risk is extremely important for the retail industry and leads to extreme compliance with AML rules.

Trust will also help with taking regulation costs into account. A principles-based approach tailored to bank specificities would reduce costs by ensuring regulation is efficiently aligned with operational realities. Conversely, a one-size-fits-all approach obliges banks to establish systems that may not align with their circumstances, thereby driving up costs unnecessarily.

Regulators should periodically conduct comprehensive cost/benefit analyses, to assess the efficacy of existing regulations and to determine whether regulatory reports remain useful or represent an undue burden on financial institutions.

The Chair summarised that achieving an appropriate balance between robustness, effectiveness and compliance costs requires strong supervisory dialogue with industry stakeholders, consistent application of a risk-based approach, and thorough cost/benefit analyses both ex ante, when preparing regulatory measures, and ex post when the measure's effectiveness has to be assessed.

6. The interplay of AML and GDPR requirements

An industry representative emphasised that harmonising AML regulations with General Data Protection Regulation (GDPR) rules is a crucial challenge. There was a recent €4.3 million fine issued to a Polish retail bank for scanning customer ID cards, which is a practice that is mandated in France under KYC procedures. There needs to be increased dialogue on and simplification of common rules for AML and GDPR to resolve inherent conflicts and ensure consistent application across Member States.

An industry representative added that there is a conflict between stringent data privacy regulations, such as GDPR, and the imperative to effectively combat financial crime. Both regulators and private sector entities share common overarching goals and could significantly benefit from strengthened public-private partnerships and an understanding of the technological opportunities.

The Chair suggested that ensuring consistency between AML regulations and GDPR is key, because of the public objectives of upholding privacy, and effectively and efficiently combating money laundering and the financing of terrorism.

7. Operational and technological challenges

An industry representative commented that there is already substantial use of AI within the industry, such as machine learning techniques that are applied to transaction monitoring (TM). Hibernation strategies of temporarily suppressing alerts for recurring low-risk patterns are utilised to avoid polluting systems with false positives and to improve overall system efficiency.

One firm's TM system, for example, proactively proposes solutions for alerts at the first-level review stage, guiding analysts towards appropriate actions based on comprehensive risk assessments. The system will even prevent the analyst from being able to close the alert.

Regulators consider such steps as cost-saving exercises, but the real driver is reducing operational risk. Even with an amazing internal academy, the analysts could each come to different decisions. What is needed is not more people but for people to perform more effectively and have a risk-based approach to alerts. Additionally, to avoid analysts being bored, they should not be spending days reviewing numerous false positives. AI helps the analysts to focus on the key risks and to not waste their time.

Agentic AI is a growing area of interest. Demonstrations revealed different AI agents were capable of autonomously extracting data from diverse sources, such as email traffic and websites, compiling information about key personnel, drafting preliminary memos that assess client risk levels, and even identifying areas for improvement in the initial assessments.

When benchmarked against the decisions current analysts would make of the risks, the results were encouraging. That then leads to questioning whether such tools could be used to automatically file Suspicious Activity Reports (SARS) to the Financial Intelligence Unit (FIU), or to stop transactions when they think there is a potential fraud. The technology presents both significant opportunities and complex challenges regarding regulatory compliance, the establishment of robust audit trails, and ensuring adequate data retention practices.

Currently, there is no idea about how regulators would assess the decision of an AI agent to redraft a memoir, for example. It is not known what freedom the industry has to use agentic AI. However, it is important to use, given the sophistication of modern money laundering operations. Money launderers are no longer limited to traditional methods like physical cash smuggling and are increasingly utilising advanced technologies and outsourcing to cross-border operations with substantial resources and expertise. Not all the smart engineers are on the right side of the law. There are very talented data scientists working for cartels and other criminal organisations, and they have been acting cross-border for a long time.

AI is already being utilised to illegitimately open accounts. Sophisticated players generate false profiles with pictures and even small businesses. There is an urgent need to proactively embrace emerging technologies to maintain an equal footing in the ongoing fight against financial crime.

Time is being wasted and there is a need to be able to act more quickly. A regulatory framework is needed, and answers to the questions about how technology can be used have to be provided so it can be implemented. Effective money launderers will initially appear as low-risk customers during the screening process. They can conceal their illicit activities by mixing them with the activities of previously legitimate businesses.

The problem of money laundering is complex, and technology is needed to help with it. There also needs to be a risk-based approach to focus on the key risks faced, and knowledge of how technology can be leveraged.

8. Closing remarks

The Chair summarised the recurring themes that emerged. The first concerns the application of a risk-based approach across all topics considered. The second significant theme relates to ensuring consistency between AML regulations and GDPR.

Regarding convergence, panellists highlighted the importance of assembling good quality people and establishing collaborative working methods between the national competent authorities and AMLA. This includes involving representatives from national authorities, which will be crucial for the AMLA's ability to achieve convergence and reach a common culture. Technology was also identified as a key factor in facilitating convergence. Regarding compliance costs, a central point raised was the necessity of prioritising simplicity during initial design phases rather than attempting to reduce complexity retrospectively.

These considerations are all part of AMLA's thinking. AMLA will operate under the principles of better regulation, and it will be conducting cost/benefit analyses and public consultations. Maintaining constructive dialogue with industry on policy and supervisory matters is considered particularly valuable.

Regarding technology, it is essential to remain ahead of technological advancements, especially given the evolving tactics employed by criminal organisations. Although there are challenges inherent in this pursuit, there should be increased speed and proactivity. Addressing potential conflicts between GDPR requirements and the effective use of technology will be vital and necessitate careful consideration of how to balance data protection with operational efficiency.