SUPERVISING AML IN CRITICAL INTERFACES

DERVILLE ROWLAND

Executive Board Member – Anti-Money Laundering Authority (AMLA)

From rulebook to reality: tackling money laundering and terrorism financing

Europe's new anti-money laundering framework, with AMLA and the Single Rulebook at its centre, responds to a simple reality: financial crime is cross-border and fast-moving.

The Single Rulebook alone does not guarantee a unified AML/CFT system. Success won't be measured by the legislation's adoption, but by AMLA's ability to turn a shared legal framework into a genuinely consistent supervisory and AML/CFT practice across the Union.

AML/CFT supervisors, FIUs, prudential supervisors, and other authorities must work closely together, informed by the best information available, to develop a holistic approach. AMLA drives this convergence by setting common rules building a shared understanding of risks, and aligning supervisory approaches.

Through this work, AMLA helps supervisors identify vulnerabilities earlier, direct resources towards the areas of greatest exposure, and take targeted and proportionate action.

AMLA builds its approach around four principles:

1. Risk based, outcome-focused and proportionate supervision
2. Strong governance and common ALM/CFT culture
3. Consistent, data-driven and technology-enabled supervisory approaches
4. Effective cooperation across the AML/CFT Supervisory System

Risk-based approach. The risk-based approach is at the core of AMLA's AML/CFT framework. Targeting supervisory resources where they are most needed requires a common methodology and shared understanding of risk. AMLA is establishing this harmonised framework for assessing ML/TF risks, creating the conditions for more consistent supervisory prioritisation and risk-based action across the Union.

Governance and culture. AMLA places governance and organisational culture at the centre of effective AML/CFT frameworks. Formal compliance alone cannot deliver effective outcomes. Obliged entities must establish clear accountability, support informed decision-making and ensure sustained engagement from their governing bodies and senior management. Through regulation, and its direct and indirect supervision, AMLA will reinforce high governance standards and foster a common supervisory culture across the EU AML/CFT system.

Data and technology. AMLA promotes the effective use of timely and accurate and information to help supervisors identify vulnerabilities, emerging typologies and act consistently across borders.

Automated and AI-based solutions can enhance risk identification while cross-border data sharing can further improve the detection of suspicious activity. However, technological innovation also creates new ML/TF typologies with increasingly sophisticated methods of concealment. The use of AI and other automated tools introduces risks where off-the-shelf solutions are introduced without adequate understanding or calibration to an institution's specific risk profile.

AMLA will support supervisors and FIUs in making responsible and effective use of these tools and foster the development of supervisory technology. It will also promote robust safeguards, sound governance and appropriate human oversight to preserve trust, accountability and effectiveness.

Cooperation. AMLA delivers its mandate through close and sustained cooperation. Common standards and a shared understanding of risk are built on timely and effective information sharing among Supervisors, FIUs, EU institutions and bodies, and the private sector.

AMLA also brings relevant partners together on cross-cutting issues such as data, technology and supervisory infrastructure. By working with the Commission, the ECB, the ESAs and other relevant bodies, AMLA helps align expertise, streamline data collections to reduce duplication and strengthen the EU's collective capacity.

A framework that evolves

Financial crime does not stand still, and neither will AMLA's supervisory approach. The principles are built to adapt risk-based supervision that recalibrates as risks evolve, governance expectations that keep pace with how obliged entities operate, data and technology that surface emerging patterns early rather than simply recording them, and cooperation that keeps the whole system moving together.

Turning the Single Rulebook into a consistent supervisory reality is not a one-off exercise. It is a forward-looking, cooperative undertaking that will evolve as risks, technologies and typologies change. AMLA's role is to keep National Competent Authorities, Financial Intelligence Units, EU-level supervisors and the private sector aligned around this shared task, so that Europe's response to money laundering and terrorist financing becomes not just more consistent, but more effective, over time.

ANDREAS SCHIRK

Head of Division, Prevention of Money Laundering and Terrorism Financing Division – Austrian Financial Market Authority

From rules to outcomes: Making European AML supervision work in AI & Crypto Era

The establishment of AMLA marks the beginning of a new phase in European AML/CFT supervision. The Single Rulebook provides the foundation, but effective and consistent supervision will require more than harmonised rules. Success will depend on close cooperation between AMLA, national competent authorities (NCAs) and the private sector. Together, they must build a supervisory model that combines convergence with flexibility, leverages data and technology, and scales solutions that work across Europe.

Convergence in supervisory expectations and outcomes is a priority. However, it takes time and standards alone will not do the trick. A common rulebook is necessary, but only one building block. Convergence also requires common methodologies, coordinated practices, effective information sharing, interoperable technology, joint training and staff exchanges. Structured cooperation between AMLA and NCAs, complemented by stakeholder dialogue, can help ensure that expectations are practical, risk-based and understood across the market. Experience from European banking supervision shows that a common supervisory culture is built through cooperation and shared practice rather than regulation alone.

At the same time, convergence should not come at the expense of supervisory effectiveness. NCAs need sufficient flexibility to address local ML/TF risks and respond to innovation effectively. Risk exposures differ across jurisdictions, from cash-intensive sectors to international financial centres, payment firms or crypto services. Input from stakeholders close to market developments can help keep supervisory responses proportionate, targeted and operationally meaningful. The objective should be convergent supervisory outcomes within a common European framework, rather than uniform supervisory processes in every situation.

AMLA can create significant European value added by addressing challenges individual authorities cannot tackle effectively on their own and by scaling successful solutions across the Union. This is particularly relevant for crypto-assets, where transactions move seamlessly across borders and supervisory insights are often fragmented. Several NCAs are already developing innovative analytical tools and supervisory technologies. AMLA should act as a platform that identifies, connects and scales such initiatives. It should evolve into a European hub for blockchain analytics and risk intelligence, interconnecting data and analytical capabilities to give supervisors a shared understanding of cross-border crypto-related ML/TF risks and emerging typologies.

> **Common rules only work if turned into shared data, tools and supervisory practice.**

Risk-based supervision must become more data-driven, with AI used to augment expert judgement. As financial services become more digital and interconnected, traditional approaches relying heavily on periodic assessments are reaching their limits. Better data, analytics and information sharing can help supervisors identify risks earlier, allocate resources more effectively and focus on areas of greatest concern. AI can further support the detection of complex patterns, improve risk identification and help process large datasets, contributing to greater consistency and efficiency. But safeguards remain essential: explainability, transparency, accountability and human oversight are needed whenever models influence supervisory assessments or compliance decisions.

Closer cooperation with the private sector will also be essential to learn and level up. Supervisors and firms face many of the same challenges when dealing with new technologies, emerging risks and evolving typologies. Structured dialogue, joint learning formats and controlled experimentation can help AMLA, NCAs and firms build practical understanding, identify safeguards and scale good practices more quickly, while respecting supervisory independence and confidentiality.

Ultimately, the future effectiveness of European AML/CFT supervision will depend less on additional rules and more on turning data, technology and cooperation into operational outcomes. Common standards remain fundamental, but they must be complemented by shared tools, shared intelligence and a shared supervisory culture. If AMLA, NCAs and the private sector cooperate effectively, Europe can build a framework that is more consistent, more proportionate and better equipped for the challanges of the AI and crypto era.

ALEXANDRE DIERS

Deputy Chief Compliance Officer, Member of the Development Committee – La Banque Postale

AI in financial crime: weapon or shield?

Artificial intelligence (AI) is reshaping the landscape of anti-money laundering (AML) and counter-terrorist financing (CTF) efforts. On the one hand, criminal organizations leverage AI to refine their fraudulent strategies; on the other, financial institutions and European regulators harness it as a powerful defensive tool. This duality challenges Europe's ability to reconcile innovation, security, and ethical considerations. By examining emerging threats, the banking sector's operational responses, and the evolving regulatory framework, we explore how the AML Authority (AMLA) and the EU should transform this challenge into a winning strategy.

AI as a crime multiplier

Criminals are increasingly exploiting AI to circumvent surveillance systems. Through deepfakes and automated bots, the production of fraudulent identities has reached industrial scale, rendering traditional controls ineffective. In 2023, the French Prudential Supervision and Resolution Authority (ACPR) reported a 40% surge in phishing attempts targeting automated systems, driven by criminal groups specializing in the fraudulent use of these technologies. By lowering costs and technical barriers, AI has democratized access to sophisticated methods formerly reserved to State actors.

AI also boosts the sophistication of money laundering schemes. In the physical world, algorithms create ephemeral legal structures to hide one's tracks: according to Europol, 60% of shell companies used in 2022 were generated via automated platforms. In the digital world, automated opening and running of pass-through accounts, privacy mixers for crypto-asset transactions, or smart contracts, provide multiple new avenues for anonymizing transactions and evading sanctions.

This transformation demands heightened and proactive vigilance from financial institutions.

AI as a compliance lever

To counter these threats, banks are integrating AI into their monitoring and alert management systems. Machine learning models analyse transactional behaviour in real time, significantly reducing false positives. For instance, La Banque Postale achieved a 60% reduction in errors when filtering name matches against people subject to restrictive measures. Graph-based analysis of transactions and relationships – notably on blockchains – has become a standard tool for uncovering hidden links between entities.

Agentic AI can now improve both the speed and quality of analyses. However, these technologies do not replace human judgment; they rather augment it. AML officers must understand how to use AI tools effectively, "feeding" them with their professional expertise to receive intelligent support and become an "augmented human".

This shift is redefining compliance roles, transforming analysts into "AI supervisors". Faced with a skills shortage, the sector must rethink training and employee support, integrating social dialogue and continuous skill development.

Along with the internal use of AI, banks also contribute to mitigating AI risks by informing and educating their clients about new fraud technologies, fostering constant vigilance while maintaining trust. La Banque Postale engages daily with its 18 million customers to this end.

An evolving European regulatory framework

While the AML/CFT regulation does not explicitly address AI systems, national authorities – such as ACPR in France – have acknowledged their relevance. White papers, workshops, and partnerships reflect this commitment to supporting the banking sector. The AMLA should now assume this role at the European level to meet two imperatives: regulatory predictability in a rapidly changing environment, and the alignment of requirements with operational realities.

This framework aims at avoiding too burdensome rules while closing loopholes exploited by criminals. The governance framework for banks, as exemplified by the Caisse des Depots Group's 2025 common position on AI use in AML/CFT, is a case in point. Beyond governance, the AMLA will need to clarify its expectations regarding the auditability and reversibility of systems, to reconcile innovation with risk management.

Europe should adapt regulation and lead emerging threats detection across the industry.

The dialectic between AI as a threat and as a compliance tool illustrates the ongoing arms race in AML/CFT. Through AMLA, Europe is laying the groundwork for a dynamic balance: recognizing AI as an indispensable yet strictly regulated lever, hybridizing skills, and strengthening cooperation between public and private actors.

The success of this approach will depend on financial institutions' ability to invest in training and collaborate with regulators. It is now up to the European Union to demonstrate that its model – combining rigor and agility – can prevail in this endless competition.

BRENT MCINTOSH
Chief Legal Officer & Corporate Secretary – Citi

Winning Europe's fight against financial crime requires partnership & prevention

Europe's move toward greater anti-money laundering convergence through the creation of the Anti-Money Laundering Authority is a welcome step toward strengthening the integrity of the European financial system. For many years, AML supervision across the European Union has been fragmented and insufficiently risk-based. AMLA should serve to promote a more harmonized framework and refocus supervision on the prevention of financial crimes across the Single Market.

As Europe strengthens its AML framework, it is important to remember the ultimate goal: preventing criminals from exploiting the financial system. Too often, regulators measure their impact by the number of findings and the size of penalties, rather than by their fundamental success in forestalling bad acts in the first place. The latter is harder to measure and may not bring the same public recognition, but it is the raison d'etre of financial crime regulation. Accountability and enforcement remain essential, but they should always be in service of outcomes such as disrupting illicit networks, identifying emerging risks and making it harder for criminals to move and hide funds. A risk-based, outcomes-focused approach helps direct supervisory efforts to the areas of greatest financial crime risk and supports the integrity of the financial system.

This is all the more important because the fight against illicit finance extends beyond Europe's borders. Criminal networks, sanctions evaders, terrorist financiers and other illicit actors operate globally, exploiting regulatory gaps and rapidly adapting to new technologies and controls. AMLA has already recognized the importance of stronger information-sharing and closer cooperation among supervisors, financial intelligence units and the private sector. Building on these commitments to share timely intelligence and foster a common understanding of emerging risks will be critical to ensure Europe can respond effectively to increasingly sophisticated threats.

Global financial institutions such as Citi will be invaluable partners in this endeavor. Banks have invested significantly in advanced monitoring systems, data analytics, artificial intelligence, and dedicated financial crime and threat intelligence capabilities. These resources enable institutions to identify suspicious activity across regions, detect emerging criminal typologies, and spot patterns that may not be discernible within a single jurisdiction. Because global banks operate across interconnected markets, they often possess unique insights on how illicit actors move funds through the international financial system and how to deter those movements.

Where effective legal frameworks and trusted partnerships exist, financial crime intelligence can be shared more effectively, helping to allocate resources efficiently. Article 75 of the AML Regulation is a significant step in this direction, providing a new basis for information-sharing partnerships across the financial sector. Combined with AMLA's focus on cooperation and supervisory convergence, Article 75 presents an opportunity to strengthen collective understanding of financial crime risks. Effective supervision is at its strongest when authorities and firms share a common view of emerging threats, vulnerabilities and typologies, allowing both supervisory approaches and risk management frameworks to evolve alongside the threat landscape.

AMLA has signaled its commitment to building a modern, intelligence-led and future-focused supervisory framework. As financial crime risks evolve alongside new technologies, maintaining this focus on innovation will be essential. The responsible use of advanced analytics, artificial intelligence and data-driven approaches can strengthen both supervision and financial crime prevention. Combined with a culture of continuous improvement and adaptability, this can help Europe's AML framework remain effective against increasingly sophisticated criminal threats.

Public-private partnerships are key to a stronger, integrated fight against financial crime.

Preventing criminals from exploiting the financial system is an objective shared by authorities and industry alike. The EU's new AML framework provides a foundation for achieving that goal, but proof of the pudding is in the tasting. Continuing to foster true partnerships between the public and private sectors will best provide Europe with the opportunity to build a more integrated, effective and resilient framework for combating financial crime.