AML CHALLENGES RAISED BY AI, CRYPTO AND DIGITAL TECHNOLOGIES

ANTE ŽIGMAN

President of the Board – Croatian Financial Services Supervisory Agency (HANFA-CFSSA)

Stronger cooperation on EU level has no alternative in money laundering fight

Money laundering risks are strongly affected by current high tech trends, as usual both in positive and negative directions. We are witnessing the new and surprising as well as sought and expected outcomes from deployment and evolution of the new technologies.

Crypto assets; notoriously known as a common de-personalised asset in third party platforms, becoming regulated will over time become less comfortable toolkit for money laundering, solely by due care which via MICA framework regulates CASPs will be obliged to apply. The burden on the regulators and even more in the supervisors role is as well growing; both the education and tech expertise will be needed to perform the proper „watchdog" role over the complex and challenging composition of the service chains in crypto assets industry.

AI by far is the most effective force in the fighter's toolkit, growing in maturity and effectiveness daily, but the capacity of the supervisory teams is possibly not ready to integrate the sole availability and this aspect shall be taken into stronger focus. While the detection ability from supervisory side is growing, the criminals are investing as well in the new tools and have as well strong tech base, often faster to reap the benefits vs. The supervisors.

Financial institutions themselves are investing in the control systems, establishing the increase resilience on their own, which makes the supervisory work easier, but not less demanding, since the understanding of the tools, their effectiveness and limitations are expected to be owned by supervisory.

Examples in Transaction Monitoring point to the near or real time identifying of relevant suspicious patterns, anomalies, discovery of hidden networks of transactions not visible to classic systems. As with any high volume analysis systems, the false positives are the cost to be taken into account, where the AI is showing strong impact, reducing and enabling proper focus to relevant area to be checked by human.

Explainability of AI, demanded by overall as well as specific deployment in AML area may be the most challenging demand, which over time may hinder the supervisory capacity while the criminals will be applying the AI technology in their full power: avoiding detection by generating the deepfakes, phishing campaign, massive fake data generation at low cost, flooding the control systems with noise, under which the fraud is successfully performed etc.

The facilitation of complex AI fraud schemes across the border requires new levels of coordination; visibility and detection capacity of a single supervisory body and respective local financial institutions shall be evaluated against the advanced criminal use cases, in order to determine proper approach to increased integration and flexibility for fast action capabilities upon discovery of a criminal activities. Needles to mention, such coordination and flexibility must be built as well using the new solutions provided by AI.

Underlying foundation for the new level of coordination and cooperation must be preservation of the core fundamentals in personal data protection, preserving public trust in the financial system, regulatory and supervisory capacity, deploying prescriptive set of rules on conditions for the data sharing, limitations on the duration of the storage of such data and access rules from personnel and systems that may use them.

> **Explainability of AI may be the most challenging demand in anti money laundering area.**

Establishment of the new cross-border coordination and cooperation may be achieved only via EU institution, using the well developed processes respected and used by all Member states, which will ensure both the legal sound basis as well supervisory consistency in usage of those new layers of fighting toolkits.

The barriers of GDPR and other fundamental rights require proper analysis, careful selection and testing of control mechanisms, which shall overcome the fragmentation, which is already clear and understood weakness in fighting the new criminal capabilities. Public dialogue , open process including the key stakeholders from all social groups, rights protection circle shall be actively engaged in order to achieve the required cooperation and data exchange capabilities in fighting money laundering growth, threatened by new technologies.

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

AMLA's approach to fostering an innovation-based AML framework in a digital age

Technology is changing markets and risks.

Technology is transforming how consumers, financial institutions and supervisors operate in the financial system. Tehnological developments also reshape the modus operandi of criminals, who rapidly adopt new tools to exploit structural gaps and scale-up their shady activity. Faster transaction processing, remote client onboarding, new digital financial services and the emergence of crypto-assets have expanded accessibility for consumers but also created new avenues to launder funds and obscure illicit activity. AI, as one of the most transformative innovations, is becoming another vector of misuse, challenging traditional identity verification and customer due diligence (CDD) processes. Together, these shifts broaden both the scale and the sophistication of ML/TF risks.

Innovation and safety mechanisms must evolve together.

The new AML Regulation reflects this transformation. It expands AML/CFT obligations to new categories of obliged entities, including CASPs, and acknowledges the role of technology in reinforcing ML/TF risk mitigation. AMLA is ready to utilise this framework by seeking effective outcomes in addressing emerging risks.

An effective response to financial crime requires moving beyond a purely rules-based approach. Automated and AI-based solutions can improve risk identification across CDD, transaction monitoring, sanctions screening and other areas. Cross-border data sharing on risk, typologies and patterns can further improve detection.

These innovations, however, must be supported by strong safeguards. Transparency, explainability, data protection, and sound model governance are essential to preserve trust and ensure effectiveness.

AMLA aims to lead by example. Through investments in advanced analytics and secure information exchange platforms, AMLA's ambition is to support supervisors and FIUs with tools to face emerging risks more consistently and effectively.

Bridging the gap between fraud prevention and AML/CFT is key.

Fraud is currently one of the fastest growing threats in the EU and a major predicate offence for ML. Fraudsters are rapidly deploying new technology and move to digital world. AMLA can play a role in bridging gaps between fraud prevention and AML. First, AMLA can support the usability of harmonised analytical tools and risk assessment methodologies that capture both ML and fraud, enabling a more integrated approach. AMLA can also promote structured information exchanges between supervisors, FIUs and industry, for instance by establishing PPPs, thus helping identify cross-border patterns.

A Year Into MiCA: Early lessons from regulating a fast-moving crypto system

MiCA represents the EU's first comprehensive regulatory framework for crypto assets. It introduces prudential, conduct and AML safeguards designed to reflect the speed and borderless nature of the crypto ecosystem. The transition from fragmented national regimes to a harmonised Rulebook is a significant step.

However, one year in early signals suggest some attempts at regulatory arbitrage through forum shopping, with a risk to maintain weak AML/CFT controls, inadequate risk management, opaque beneficial ownership and governance structures. This indicates the need for further harmonisation to address remaining national divergences.

New risk areas are also emerging through exposure to unauthorised stablecoins, increasingly complex token models and continual innovation in DeFi. These developments require monitoring and coordinated supervisory action.

AMLA will play a key role by driving supervisory convergence on AML expectations for CASPs, strengthening cross-border coordination, enhanced data sharing and alignment between AML and MiCA frameworks.

Effectiveness is the core objective.

Achieving consistent and effective supervisory outcomes across the Union requires a shared understanding of emerging risks, the convergence of supervisory expectations and actions, and stronger information sharing mechanisms than exist today.

A genuinely data driven, risk-based approach can only be realised through sustained investment in technology. This includes advanced analytics and a SupTech-ready supervisory infrastructure capable of enabling continuous monitoring, secure cross-border data exchanges, and more dynamic responses to evolving ML/TF threats. Innovation is a prerequisite for effectiveness.

By fostering supervisory convergence and coordinating the EU FIU system, AMLA will contribute to a more effective financial crime prevention system. AMLA's integrated data ecosystem, including its forthcoming EU wide AML/CFT database, will provide a common foundation for more harmonized, intelligence led supervision.

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

Strengthening AML supervision in an AI- and crypto-enabled financial system

Artificial intelligence (AI), crypto-assets and digital platforms are reshaping money laundering (ML), terrorist financing (TF) and financial sanctions evasion risks in ways that require supervisors to rethink how risks emerge, scale and interconnect. From a supervisory perspective, the rapid evolution of ML schemes, the ability of crypto-assets to move funds automatically across chains and intermediaries, and the automation of illicit transactions through AI are fundamentally changing both the velocity and opacity of criminal activity, including the rapid circumvention of financial sanctions frameworks.

Crypto-assets in particular compress distance and jurisdiction: value can be transferred across borders within seconds, split into micro-flows, routed through multiple service providers and reassembled elsewhere. This creates structurally higher ML/TF risks, especially where mixers, privacy-enhancing technologies or unregistered service providers are involved. These dynamics are also increasingly used to evade financial sanctions, for example by routing value through high risk jurisdictions, privacy enhancing technologies or decentralised exchanges that fall outside traditional perimeter controls. For national supervisors, this means traditional case-by case analysis is no longer sufficient; we need system-level visibility over blockchain flows and typologies.

AI amplifies identity and network risks. Synthetic identities, deepfake impersonation and automated onboarding attacks increasingly target the seams between human judgement and system thresholds. Meanwhile, automated transaction chains – often running 24/7 – leverage mules, OTC desks and cross asset bridges, making ex post reconstruction extremely resource intensive.

The core AML/CFT framework remains sound, but the operational capabilities are not yet calibrated for real time, cross border ML/TF in an AI enabled environment. As in other supervisory areas, we need to further step and scale up data driven supervision. At the FMA, this includes the development of SupTech tools for analysing crypto transaction flows and identifying emerging ML patterns – work that can feed into a broader European solution.

The rise of crypto related ML/TF risks makes a European blockchain analytics capability not just useful, but indispensable. Fragmented national tools cannot substitute for a shared analytical infrastructure that provides supervisors and FIUs with consistent, high quality insights across chains, jurisdictions and service providers. AMLA will be uniquely placed to help build and operate such a capability, ensuring interoperability, common data standards and the ability to detect cross border risks early. The FMA is actively contributing its experience to support this work.

Better data alone is not enough. The EU's AML package introduces new forms of public–private partnerships ('partnerships for information sharing') that can significantly enhance ML/TF detection when implemented effectively. For supervisors, this means ensuring that information-sharing partnerships operate on a solid legal basis, respect fundamental rights, and deliver timely, actionable intelligence. Together with other supervisory authorities the FMA is working to foster such structures at both European and national levels and sees value in AMLA supporting consistent implementation across the EU.

To strengthen overall effectiveness, three levers are central. First, shared data with safeguards – common standards, privacy preserving analytics and secure channels for exchanging information with FIUs and obliged entities. Second, automation with accountability – making broader use of AI based analytics, graph models and anomaly detection, while maintaining explainability and human oversight for high impact decisions. Third, clearer incentives and responsibilities – predictable consequences for persistent weaknesses and safe harbour mechanisms that encourage rapid information sharing and early intervention.

> Stronger data, shared tools and coordinated action are key for AI and crypto era AML/CFT.

The convergence of fraud and ML, particularly through crypto assets, reinforces the need for end to end controls: onboarding checks capable of detecting synthetic identities, beneficiary verification, monitoring of crypto off ramps, and rapid freezing or recall capabilities. AMLA in coordination with other European agencies can add value by harmonising expectations, steering supervision of major cross border crypto and payment actors and leveraging national SupTech tools or at least ensuring interoperability.

KYC must become more dynamic as AI-enabled impersonation and scalable document fraud grow. This entails inter alia continuous verification signals and behavioural analytics. Yet effectiveness must be matched with trust: transparency on automated decisions, clear redress mechanisms and strong governance are essential.

In short, to address AI and crypto driven financial crime risks, supervision must evolve from controlling individual institutions to overseeing interconnected ecosystems – supported by strong national capabilities, shared European tools, and coordinated action.

MARC FUNGARD
Global Regulatory Compliance &
Enterprise Risk Lead – Stripe

The agentic economy: maintaining ecosystem trust with velocity

The financial ecosystem is transitioning from "digitized" to "digital-native." This era is defined by three tailwinds: agentic AI, stablecoins, and generative AI. European policymakers should modernize a 25-year-old AML/CFT framework built for physical documents and human-speed transactions because as commerce becomes even more global and agent-led, antiquated processes will achieve mere technical compliance but inhibit actual effective risk management.

Central to this shift is a broadening adoption of LLM-driven artificial intelligence 'agentic commerce', where AI agents manage and soon execute transactions on our behalf. The growing internet economy means that the "domestic market" of most new online businesses is the internet itself. This transition - from local business creation to a "global by default" micro-multinationals - is underway. Stripe is actively building the financial infrastructure to support it; major retailers are piloting agentic systems for procurement processes and consumer sales. This speed holds tremendous promise for European growth - but can be heavily impacted by well-intended, but antiquated implementation of sensible regulatory principles.

In an agentic flow, traditional KYC and SCA processes become points of failure instead of security enhancements; the demands of a human interaction coupled with a slow verification breaks the high-velocity workflows of autonomous agents. Creating ever higher barriers to entry in the formal financial system risks creating commercial incentives to move into unregulated, shadow ecosystems which will operate faster and cheaper, but without regulatory guardrails. This will expose customers to more risk, impede law enforcement, and worsen financial inclusion. Identification, authentication, and verification must adopt standards that leverage the abilities of the technology. Agents don't have passports.

While agentic flows can work in any currency, the global nature of the activity will likely mean that much of the future of commerce will run on stablecoin rails - which operate globally, 24/7, and settle instantly and autonomously. Financial crime detection has always suffered from time lag - SARs are filed long after the actual suspicious incident; in an agentic and stablecoin world, they are outdated. The velocity of the digital assets can instead be strength: programmable capabilities, close coordination with governments, and better upfront verification and monitoring can potentially stop illicit funds in real-time - and enhance financial inclusion.

The rise of generative AI has effectively "broken" the primacy of digitised physical documents. Deepfakes and synthetic identities now bypass traditional verification with ease; human accuracy in detecting these frauds has plummeted to 24.5%. To future-proof the Single Market, we must move beyond the static document. While the EU's leadership on e-IDAS is vital, we need a hybrid model that merges "how you behave" and "what you hold," layering cryptographic proofs with real-time behavioral signals like device telemetry. This shift from "artifacts" to "signals" is the only way to defend against the scale of generative fraud.

Agentic commerce, stablecoin settlement and generative identity each offer challenge and opportunity to core AML implementation and operations, but do not change the goal of a safe, secure system for citizens. Onboarding must verify delegation credentials, agent provenance, and human identity; monitoring must model behaviour real-time, to cope with high-velocity, fragmented flows. Our experience building scalable, model-driven detection shows the practical value of embedding intelligence into transaction flows rather than relying solely on post facto review.

Finally, the greatest risk to European financial stability is fragmented intelligence. Crime networks have never respected borders; today, they do so at the speed of AI. The establishment of the Anti-Money Laundering Authority (AMLA) alongside the Instant Payments Regulation (IPR) and Payment Services Regulation (PSR) are key steps. However, we must champion a unified, API-led standard for intelligence sharing—similar to EBA Clearing's FPAD—over fragmented national silos. Europe's competitive edge in the AI era will be defined by its ability to share data at the speed of the threat.

The growing internet economy means that the "domestic market" is the internet itself.

As agentic commerce, stablecoin settlement, and generative identity redefine the financial ecosystem, the transition toward a regulatory model of supervised autonomy becomes essential. By prioritizing unified intelligence and embedded safeguards, the nature of these digital-native flows can be transformed from a systemic challenge into a structural advantage for the Single Market.

BEATRICE COSSA-DUMURGIER
Chief Executive Officer, Western Europe – Revolut

A harmonised, risk-based AML framework to help EU banks scale safely and effectively

Digital finance and emerging technologies like AI are transforming how banks operate, with instant payments, digital onboarding, and cross-border platforms that have compressed timeframes and expanded scale to respond to customers' demands. Criminals have adapted just as quickly, with increasing money laundering activities and online fraud, in a financial ecosystem that is more efficient, but remains vulnerable.

AI illustrates this dual reality. It significantly enhances behavioural monitoring, anomaly detection, and network analysis, helping identify mule accounts, suspicious patterns, and complex layering strategies in near real time. Yet the same technologies can be weaponised by criminals to generate synthetic identities, automate phishing, or mimic legitimate behaviour. The challenge is not whether to use AI, but under which parameters. Clear regulatory guidance on deployment, transparency, and accountability is essential to maximise defensive capabilities while limiting misuse.

These capabilities highlight that emerging technologies do not operate in isolation: the risks they detect or create ripple across the entire financial ecosystem, making cooperation and integrated AML strategies essential. Fraud and money laundering are now deeply interconnected and criminal proceeds are routed instantly through payment accounts, crypto gateways, or cross-border transfers. A fraud case can become a money laundering case within minutes. Cooperation and information sharing across the entire fraud and AML chain: banks, payment service providers, fintechs, Financial Intelligence Units, and law enforcement, are therefore indispensable. In this regard, the establishment of AMLA will enhance pan-EU AML/CFT supervision by directly overseeing cross-border financial entities, coordinating national authorities and FIUs and issuing common regulatory standards.

Because fraud and money laundering exploit the weaknesses of multiple actors simultaneously, the most effective response combines data sharing, automation, and clear liability regimes. Real-time information exchange between institutions and public authorities has proven one of the most powerful tools to detect mule networks and coordinated fraud schemes. Similarly, shared risk indicators and operational feedback loops improve detection and reduce false positives. Automation helps prioritise alerts, process rich datasets, and enable earlier intervention, freeing human expertise for complex cases.

Yet even with advanced tools and clear responsibilities, the operational effectiveness of AML measures can be undermined by fragmented regulation and diverging expectations across jurisdictions. For fast-growing digital banks, the tension is not between innovation, customer experience, and AML compliance. Robust controls are a core enabler of trust and platform security. Customers expect services that are instant and safe. Divergent reporting formats, interpretations, and feedback loops on the other hand slow operations without improving risk outcomes.

Past experience with PSD2 illustrates the concrete consequences of partial harmonisation. While it strengthened strong customer authentication and transformed European payments, PSD2 could not fully curb new fraud types, such as more sophisticated authorised push payment fraud, and its fragmented implementation left loopholes exploited by criminals. PSD3 and the new Payment Services Regulation (PSR) have therefore never been more timely in addressing these gaps with harmonised anti-fraud rules and clearer responsibilities across the fraud chain, shifting the ecosystem from reactive defence to shared prevention.

The challenge for cross-border banks is fragmented regulatory enforcement & supervisory expectations.

Ultimately, the goal is not simply compliance, but building a coherent ecosystem that is resilient, trustworthy, and capable of scaling innovation safely across Europe. Fraud and money laundering are ecosystem risks that cannot be addressed in a siloed way, as they do not affect isolated institutions, but the entire financial system and consumer trust, for which public-private cooperation and regulated intelligence-sharing mechanisms are indispensable. Europe now has a unique opportunity: by ensuring its AML and anti-fraud framework is harmonised, risk-based, and technologically neutral, it can strengthen resilience while enabling digital innovation to scale safely across the Single Market.