AML challenges raised by AI, crypto and digital technologies

1. An industrialised, borderless threat calls for a return to fundamentals and system-wide supervision

1.1 The industrialisation of money laundering: regulating new tools by going back to basics

A supervisor opened by noting that money launderers' exploitation of AI, crypto and instant payments has accelerated beyond what traditional frameworks can track. A supervisor confirmed that laundering is industrialising, with the pandemic as the turning point: fraud now represents 40% of FIU's suspicious activity reports (SARs), against 20% five years ago, with at least 10% involving AI-enabled impersonation; mule accounts feature in 80% of the account numbers cited in SARs; and crypto, once negligible, now appears in 20%. He argued the right response is, counterintuitively, to go back to fundamentals — analysing new instruments by reference to existing frameworks — citing MiCA and the Transfer of Funds Regulation as good examples and stressing the importance of timeliness. An industry representative confirmed that AI is an operational reality at Revolut, where deepfake-related verification attempts rose 180% in 2025, exposing the fragility of static onboarding; AI deployed defensively has multiplied the productivity of FinCrime agents tenfold, but human judgement remains essential. A supervisor observed that, as soon as one vulnerability is closed, another emerges. A supervisor added that synthetic identities and round-the-clock automated transaction chains often delay detection past the point of intervention.

1.2 Borderless reach and compressed timelines: from case-by-case to system-wide supervision of interfaces

An industry representative noted that crypto assets, often originating in high-risk jurisdictions, add layers of complexity that challenge the follow-the-money approach: although the illicit share of overall market capitalisation remains low, the complexity of these flows has risen sharply. MiCA has provided welcome legal certainty, and AMLA's single-window supervisory approach will help close gaps for legitimate crypto-asset service providers, with traceability and international cooperation as priorities. A supervisor recalled that money laundering itself is not new, but the reach afforded by billions of mobile devices is — illustrated by a recent supervisory case involving people in their eighties used as mules through a crypto-asset provider, showing that criminals exploit technology both directly and indirectly through unwitting individuals. A supervisor observed that crypto compresses distance, space and jurisdiction, and that the payment chain has been transformed: fraud proceeds move through crypto ATMs into fiat, via instant payments back into crypto, then out again. The supervisory response must concentrate on interfaces — between crypto and fiat, between humans and AI, and between frameworks and jurisdictions — and abandon the case-by-case, follow-the-money approach in favour of a holistic, network-level view.

1.3 State actors and professionalised theft: predicting AML risk through threat-vector intelligence

An industry representative explained that Fireblocks brings a different angle: as a custodial-technology provider for regulated custodians inside and outside the EU, its work focuses on preventing thefts rather than tracing them, by identifying vulnerabilities in wallet infrastructure that perpetrators exploit. Recent analytics show a 600%-plus surge in the value received by sanctioned digital-asset wallets — described as the next stage of maturity in AML risk for digital assets. The largest single-event thefts, ranging from USD 1 billion to USD 3 billion, can be traced to state actors — most notably the DPRK — exploiting long-standing vulnerabilities. She called for closer collaboration between the AML community and threat-vector specialists, sharing intelligence on emerging attack typologies including man-in-the-middle attacks, attacks on API endpoints by AI agents, and the exploitation of blind signing — where a sender believes they are transferring assets to a known counterparty but is in fact sending them to a third party. Categorising criminal exploits enables better prediction of which actors are likely to steal funds and what their first laundering moves will be. With the timeline between exploit and laundering both vastly professionalised and dramatically compressed, the supervisory window is narrowing; detecting actors and their preferred patterns allows earlier prediction of AML risk.

2. Fragmented supervision and operational gaps demand coordination, scaling up and hybrid skills

2.1 Closing the regulatory-arbitrage gap through borderless coordination and the single AML rulebook

A supervisor framed the second part around whether existing frameworks are equipped for the pace of financial crime. A supervisor warned that launderers exploit regulatory arbitrage and uneven implementation across jurisdictions — illustrated by ATMs, once bank-operated but now widely deployed by crypto-asset providers — and conceded that supervisors are not yet sufficiently equipped. He saw immediate scope for stepping up coordination between AMLA, EIOPA, ESMA, NCAs and

international counterparts, requiring goodwill rather than new investment. AI systems gravitate to weaker-enforcement jurisdictions and exploit below-threshold transactions; supervisors should avoid duplicative data requests on firms. A supervisor suggested that the best coordination is the kind that does not need to take place: digital criminality is borderless, supervisors must follow, and placing major European CASPs under AMLA's direct supervision would deliver clear added value. He challenged the view that criminals are always ahead — banks often lead innovation, and regulators, as referees, can adapt the rules. An industry representative noted that, although European AML standards rank among the highest globally, divergent national approaches and predictable processes — paper-based proof of address, randomised on-threshold monitoring, varying cash-ID limits — are exploited by criminals; the single AML rulebook and AMLA will harmonise enforcement.

2.2 Operational lag and fragmentation: scaling up shared analytics and SupTech investment

A supervisor noted that, while the regulatory direction is right and continues to improve, operational capabilities have not yet caught up with AI-enabled, real-time, cross-border laundering: significant work has been done on the operational side, less on the legal-regulatory side. Smart solutions and the new AMLA platform should support collective scaling-up. Crypto's blockchain traceability is well understood, but the full picture only emerges at European level — fragmentation is the priority, with shared analytical capabilities central. He concluded that the regulatory framework is where progress lags most, and that sharing technology and the expertise to use it will be decisive. An industry representative illustrated industry scaling: Revolut operates fluidly across 27 countries on a single platform, allowing cross-border patterns to be identified more readily. It onboards one million customers every 17 days, serves 70 million globally — 50 million in Europe — and dedicates over a third of its 13,000-strong workforce to AML, with a central investigation unit for complex cross-border cases. With cross-border electronic payments and embedded finance accelerating, human review alone is no longer enough: real-time AML controls must be implemented, supported by pre-calibrated, behavioural-analytics-based risk models, in a layered architecture combining strong ex ante prevention with strong ex post intelligence.

2.3 AI manipulation of humans and systems: human-in-the-loop oversight backed by hybrid skills

A supervisor argued that human-in-the-loop oversight must evolve in both public and private sectors to make full use of AI tools: AML expertise alone will not suffice. Individuals and organisations alike must develop hybrid skills, and supervisors should collaborate and learn from one another on the job to keep pace with criminal innovation. An industry representative welcomed the prospect of stronger European coordination and information sharing, offering Fireblocks' role as an analyst of attack typologies and threat vectors as one input. She drew particular attention to the use of AI to manipulate humans — already illustrated by other panellists — and to a newer dimension: the use of AI to manipulate the system itself. As AI agents become increasingly autonomous, attackers may interfere with them by manipulating prompts or training data, giving rise to system-to-system vulnerabilities in addition to the AI-to-human-to-system vulnerabilities seen until now. As supervisors coordinate, learn and adapt their skills, they should make systematic use of system reviews with supervised entities and embrace automation as a means of countering the automated vulnerabilities that an increasingly AI-based financial system will produce.

3. AML effectiveness, efficiency and customer trust are not a trade-off, provided controls become targeted, embedded and explainable

3.1 Fewer blunt controls, more targeted ones: rebuilding trust through explainability

A supervisor summarised that, despite the alarming pace of criminal evolution, innovative tools and the dedication of the industry will help combat illegal activity, with public-private cooperation key. He framed the third part around reconciling AML effectiveness with the customer experience, given how directly trust feeds back into the effectiveness of preventive measures. A supervisor argued that the framework needs fewer blunt controls and more targeted ones: customers blocked or off boarded because of fragmented information or de-risking lose confidence in the system, while the criminal networks that sometimes exploit those very customers remain active. He highlighted three considerations. First, cooperation between supervisors, FIUs and obliged entities must be intensified, with the AML regulation's information-sharing provision used in good faith and without indiscriminate data dissemination. Second, sharing analytics and technology requires a clear explainability threshold — AI is now widely used, but if the basis for high-impact decisions such as blocking or off-boarding cannot be clearly articulated, the legitimacy of the system will be called into question, making well-trained humans-in-the-loop indispensable.

3.2 Embedded automation and event-based KYC: adapting to an AI-driven economy without becoming a black box

A supervisor, continuing his three considerations, concluded that KYC should evolve into a dynamic, event-based verification process; any use of behavioural analytics in this area must be clearly explainable and justifiable to both supervisors and the public, in order to safeguard trust. An industry representative suggested that, in the face of increasing complexity and speed, compliance must become embedded and automated. Whitelists and blacklists can control where assets may or may not be sent; transactions can be screened in real time as they are sent; wallet infrastructures can be integrated with AML tools and scanning techniques so that compliance checks happen seamlessly. This is, in practice, the only way for financial institutions to adapt to a faster, more complex and more AI-driven economy. At the same time, automated and embedded compliance

must not appear to supervisors as an inscrutable 'black box'. Echoing supervisor´s earlier point, she noted that the only way to win is to play the game where it is being played — and the game is moving towards automated processes. Supervisors and industry must therefore work together to build supervisory confidence around automation rather than discourage it; this is the philosophy underpinning Fireblocks' platform.

3.3 Effective AML with an eye on efficiency: skilled people, standardisation and a culture of cooperation

A supervisor underlined that effective AML supervision rests on human capital — experts in big-data analytics, not least within AMLA itself — and on standardised corporate-sector data, since non-comparable data is exploited by criminals. AML controls must also protect the AML system against cyber-attacks. An industry representative emphasised there is no trade-off between proper AML compliance and an optimal customer experience: customers expect both speed and safety. Banks must cut false positives, avoid unnecessary de-risking and collect only proportionate data. The industry needs greater legal certainty on cross-border data processing and sharing — privacy should not shield criminals — while GDPR uncertainty hampers the sharing of suspicious-transaction information; cultural and reputational barriers must also be addressed. A supervisor stressed that effectiveness must be matched by efficiency: a thematic review of ten domestic largest banks identified hundreds of millions of euros of direct AML costs. Just as supervisors should be technology-neutral, innovators must themselves be neutral or friendly to compliance. A supervisor closed by noting that deepfakes, mule accounts and crypto-related complexity are now routine — but public-private cooperation, standardisation, industrialised preventive systems and a refusal to tolerate regulatory arbitrage offer grounds for optimism, with the investment already committed showing commitment goes beyond rhetoric.