

July | Your Monthly Compliance Brief

July 2026 marks a significant moment in EU AML enforcement, and the implications for financial institutions and their compliance infrastructure are immediate.

MiCA's grandfathering period has expired, AMLA's first batch of the Regulatory Technical Standards is due this week, and the EU's unified AML rulebook is now less than twelve months from full application.

This edition details how these regulatory developments directly affect your operations, what you'll need to demonstrate, and where your current processes may leave you exposed – alongside updates from a busy Q2 on the road across Europe and what compliant AI now looks like in practice.

Q2 Events: What We Heard Across Europe

[NDA Client] Dinners: April

April marked the start of a series of private dinners across Europe, bringing together senior compliance leaders, regulators, and financial crime professionals for closed-door conversations about where the industry is heading.

In Malta, [NDA Client] and QUBE Events gathered leading decision-makers from financial crime compliance, payments, and fintech for an evening of informal networking and meaningful conversation.

A week later, a private dinner in London brought together senior voices across financial crime, compliance, and FinTech for what proved to be a particularly candid evening, with honest perspectives on what's working, what isn't, and how to navigate the growing tension between innovation, regulation and responsibility.

Next, at Storchén Zürich, [NDA Client] hosted senior leaders from six regulated banks and financial institutions, global Tier 1 consulting firms, a leading reinsurance group, and regulated fintechs – collectively managing hundreds of billions in assets – alongside Axel Weber, former Chairman of UBS and former President of the Deutsche Bundesbank.

The questions that dominated the room: Yes, AI *can* support compliance – but how far can it go, and under what conditions can it be trusted?

What would a board need to see to approve AI in production? How should institutions engage regulators on AI deployment: proactively or after implementation? What does AI governance actually look like in practice?

The ability to answer those confidently is what holds institutions back – and [NDA Client] addressed them publicly in his interview with Financial IT at Money20/20 the following month.

Money 20/20 Europe: 2nd June – 4th June

[IMAGES: Money 20/20 – once supplied]

[NDA Client] attended Money20/20 Europe for the first time this year, with 40+ meetings with banks, fintechs, investors, and partners across the three days.

Conversations reflected a market that has matured; prior discussions around AI in financial services were about its potential. In Amsterdam, they focused on its deployment, governance, and accountability.

For cross-border fintechs, faster KYB onboarding and AML reviews are now a priority and, increasingly, CEOs are driving these conversations. The perception of compliance as a back-office function is fading, now viewed as an active enabler of business growth, and the sheer number of compliance leaders, risk professionals and financial crime experts present embodied that shift.

NextGen Payments & RegTech Forum, Dublin: 11th June

[NDA Client] sponsored the NextGen Payments & RegTech Forum in Dublin, with our Head of Marketing, [NDA Client], delivering the keynote on how financial institutions can deploy AI safely, transparently and in a way that stands up to regulatory scrutiny.

The presentation opened with a simple observation: an AI model can tell you what a business does. It usually can't show you how it got there.

Verifying what a business actually does requires deliberate, traceable steps: reviewing disclosures, tracing legal entities, validating products and services across multiple sources.

That distinction, between traditional AI that produces an answer and AI that can show its working, was a recurring theme in post-keynote conversations. And that level of explainable, 'regulator-ready' AI is fast becoming the baseline expectation.

[NDA Client] in the Press

At Money20/20 Europe, our Founder and CEO, [NDA Client], sat down with Financial IT to explore the state of AI adoption in financial crime compliance and why, despite rising industry sentiment to implement AI, boards and senior stakeholders remain hesitant.

[NDA Client] defines the biggest challenge to successful adoption as neither widespread inertia - banks and fintechs are certainly aware, with compliance costs reaching up to 15% of operating expenses - nor the technology. AI is evolving faster than traditional regulation itself, a point the FCA's own chief executive, Nikhil Rathi, made publicly just last week.

The issue is trust, the lack of which takes the form of two key questions: can AI be trusted in heavily regulated environments, and will it hold up under intense scrutiny from both regulators and auditors alike?

Alleviating that scepticism calls for transparency. Specifically, it calls for what [NDA Client] describes as 'regulator-first AI' – agents designed to meet regulatory expectations rather than retrofitted to satisfy them after the fact, and capable of adapting to the shifting ground beneath compliance teams' feet.

Taken together with the regulatory developments outlined below, this is fast becoming the baseline for financial institutions.

The Regulatory Picture: Q2 2026

AMLR: One Rulebook, One Standard

Viewed individually, the regulations as introduced as part of the EU's AML package seem to each present a different challenge for compliance teams.

When inspected further, however, they converge around the same demand: show your working. *Prove* your process. AMLR is where that demand becomes law; the connective tissue binding 27 member states to one rulebook.

The register is no longer enough

A match between the company's declaration and the national beneficial ownership register is often accepted as sufficient verification. From July 2027, that's no longer defensible.

You're expected to verify independently *first* – registry filings, articles of association, and shareholder lists – and *then* cross-reference against the register.

Should your findings differ, you're legally required to report any discrepancies within 14 days. Missing any mismatch or failing to report it is treated as two separate regulatory breaches.

The problem with relying on third-party data providers or a black-box AI system is the same: you won't know how they reached their conclusion, what sources they used, or how they calculated those UBO percentages.

Having the right answer won't satisfy regulators; you must own the underlying process, and it must be fully traceable.

How AMLR Affects Your CDD

This need to show your work now extends beyond ownership identification to PEP screening, too. AMLR significantly expands the definition of family members and close associates, two relationships that rarely appear in any register – and will require structured, documented investigation to surface.

Though changes are not limited to onboarding. Under the new guidelines, your customer data must be formally refreshed – for high-risk relationships, this is a hard cap of one year.

Just as demanding is the emergency reporting rule. If a financial intelligence unit requests an account's evidence trail, you have a maximum of five working days to hand it over, leaving no room for retroactive compliance. The inference is clear: your audit trail needs to exist already.

The Lowered UBO Threshold

The UBO threshold moves from "more than 25%" to "25% or more", closing the loophole that allowed someone holding exactly 25% to fall outside reporting definitions entirely. But how you determine who reaches that threshold in the first place is about to undergo serious change.

Three Checks

UBO mapping now requires three separate checks: ownership, control, and the combination of the two. A person can be a UBO through majority voting rights, board appointment powers, or veto rights alone, without any equity whatsoever.

Like PEP connections through family members and close associates, that person won't appear in any register. The Combination Rule catches those who own at one level and control at another within the same chain.

The Accumulation Method

Under current approaches, ownership is assessed chain by chain. Under AMLR, percentages are multiplied down every corporate layer and totalled across *all* chains.

Built to catch someone deliberately splitting a controlling stake across multiple chains to stay below the threshold in each, it calls for meticulous mapping – every holding company and every individual with capital and voting rights to be recorded.

The Threshold Is Dependent

For clients operating in higher-risk sectors – complex cross-border holding structures or chains of shell companies across jurisdictions outside EU oversight — the threshold can drop to 15%.

Individual member states can enforce this locally from July 2027, and the Commission's assessment of which sectors qualify runs through until 2029, but the system capable of adapting needs to be in place before then.

Applying the incorrect threshold, regardless of how thorough your UBO identification was otherwise, is a regulatory breach. The law becomes a moving target, and your compliance logic needs to be dynamic to keep pace, capable of analysing the client's risk profile, and then determining scope.

That level of variability leaves little room for rule-based legacy platforms built on static hardcode.

AMLA: The New Supranational Authority on European Financial Crime

Those outside of the AMLA's direct supervision may feel that they won't be subject to the same level of scrutiny as befalls those deemed higher-risk.

Companies operating across multiple European markets may hope to still benefit from relatively softer interpretations in certain jurisdictions, as they did under the previous 'patchwork' of rules stitched together by independent, national supervisors applying EU directives as they saw fit.

Yet, with AMLA perched above every national regulator in the EU and conducting ongoing peer reviews to ensure consistent application of its rulebook, AMLR, this begins to fall apart at the seams.

The lines between national jurisdictions are eroded. As local regulators begin to crack down on those within their catchment to protect their own standing, companies can expect enforcement of the rules to be altogether faster and tighter. The same compliance framework that satisfied your national regulator last year may not pass muster.

The window for adaptation is being compressed; by the time AMLR is in effect, firms are expected to have already redesigned their policies, systems and governance.

Earlier this year, Luxembourg's AED rejected nearly 90% of AML questionnaires submitted by investment firms, failures concentrated in the identification of corporate entities and UBO structures – a stark indicator of the chasm between current practices and the expected standards.

A further 68% of Annual Compliance Officer Reports were rejected due to data quality and structural gaps in how firms documented their process.

These firms didn't necessarily fail to reach the correct conclusion; they were incapable of showing and justifying how they reached it, and, under AMLA's directive, any answer that lacks the documented trail to support it, even if correct, is treated as non-compliant.

Regulators are demanding an atomic level of traceability that can only be produced automatically, in real time, by systems designed specifically for that purpose – and AMLA's incoming Regulatory Technical Standards (RTS) lay out the requirements unambiguously.

The RTS: What Compliant Systems Must Demonstrate

AMLA is currently finalising the Regulatory Technical Standards – their technical specifications, which will specify, to the letter, what compliant systems must be able to demonstrate.

They will dictate exactly what compliant systems must demonstrate: how UBO calculations must be recorded and reconstructed, what a complete audit trail looks like, and what transaction monitoring must show about every decision it makes.

And, once adopted by the European Commission, they are legally binding.

Although AMLR will not be in full effect until July 10th, 2027, the curtain is already being drawn, with the first batch due for submission to the European Commission on 10 July 2026.

We're in the midst of a transitional period; one that compliance leaders at regulated financial institutions should make full use of today to avoid exposure.

Leniency for late adapters cannot be counted upon – and any infrastructure change must occur incrementally.

The Technological Maturity Audit

Supervisory assessments now extend beyond policy reviews, with AMLA or an aligned regulator conducting data-driven inspections of your entire live production environment: the tracking logic, the source documents, and the step-by-step history behind every compliance decision your system has made.

Two gaps define where most institutions will be exposed:

Gaps Between Policy and Reality

If your compliance policy states that you assess beneficial ownership using the accumulation method across all chains, yet an auditor finds that your system only traces ownership one level deep, that gap is a severe regulatory breach. One that you, as MLRO, are personally accountable for.

Historical Reconstruction Problems

Should a regulator flag a client onboarding from eighteen months prior, they'll be less concerned about what the conclusion was, and more so about how your system reached it and whether it can reproduce the exact same answer under the specific conditions on that specific date

In each case, failure stems from the same place: a system that produces answers it cannot explain, through a process it cannot reconstruct, from sources it cannot show.

MiCA: The Expiration Date Has Arrived

The grace period to obtain a full MiCA CASP license expired on 1st July 2026.

Approximately 230 have secured their full MiCA CASP authorisation – a fraction of the more than 1,200 crypto businesses previously active under national registrations across the EU.

The remainder, whether they chose not to apply, withdrew mid-process, or await verdict, are now operating outside EU law for any new business activity.

For banks, payment institutions, and regulated fintechs maintaining correspondent relationships or providing settlement infrastructure to crypto firms, continuing to route funds to or maintain accounts for unlicensed entities exposes you to supervisory action, including transaction blocking and account termination.

The urgency for verification is equally high for those in venture capital, private equity, or corporate finance advisory roles. For any portfolio company or target acquisition reliant on European transaction volume, its ability to operate within the EU now ceases.

Auditing holdings against ESMA's centralised MiCA register is now imperative to identify and remediate any non-compliant asset exposure.

For institutions that don't consider themselves crypto-facing, the prevalent question is whether any of your payment flows, correspondent relationships, or corporate clients interact with licensed crypto asset service providers. If so, then the Transfer of Funds Regulation applies to those transactions.

The Transfer of Funds Regulation

With the EU's Transfer of Funds Regulation, every crypto asset transfer, regardless of value, must be accompanied by verified originator and beneficiary data – who initiated it, who

received it, and through which regulated entity it passed. And it applies with no minimum threshold.

Risk scores supplied by a third-party vendor will not suffice; when a transaction involves an unhosted wallet, you must independently verify who controls it and document how you reached that conclusion.

In other words, the Transfer of Funds Regulation demands at the transaction level what AMLR demands at onboarding, and AMLA is turning into a hard technical definition of what your system must be able to do via its RTS: a sequence of atomic, traceable, individually logged steps and decisions.

The EU package fundamentally changes what constitutes compliance and poses a vital but uncomfortable question for compliance leaders: are your processes still defensible under this fresh regulatory scrutiny?

Yet the picture is also changing for those outside AMLA's jurisdiction.

The FCA are 'rethinking regulation' in the face of AI

At TechUK's Events of Change conference on 24th June, Nikhil Rath, FCA Chief Executive, made clear the direction of travel for financial institutions in the UK – with distinct parallels.

The FCA, he stated, have become “as much a data and technology regulator as a financial services regulator”, signalling that, similar to AMLA's RTS, they will now also audit firms' technology as closely as they do their policy.

And, from his vantage point, it's clear where AI in financial services is headed next: past generative AI that merely summarises and detects, and toward agentic systems that coordinate and transact autonomously.

The condition Rath attached to that transition matters most. The FCA explicitly requires full accountability – with human oversight built in from the beginning. He was explicit that any dependencies on model providers, data providers, or third-party vendors must be thoroughly mapped and governed, and the Critical Third Parties regime enforces this by law.

Nikhil grounded his concerns in the UK Finance's Annual Fraud Report, which revealed that the UK lost almost £1.3 billion via payment fraud last year, with two-thirds of authorised fraud cases originating through social media and messaging platforms – with the expectation that firms assume direct responsibility to stop criminals exploiting their platforms.

The FCA are acclimating swiftly, and regulated firms would do well to adopt the same urgency.

Read the full speech here:

[\[https://www.fca.org.uk/news/speeches/rethinking-regulation-age-ai\]](https://www.fca.org.uk/news/speeches/rethinking-regulation-age-ai)

TransferMate: Defensible AI in practice

TransferMate has partnered with [NDA Client] to significantly overhaul its AML and sanctions screening operations, whilst retaining full auditability and strict human-in-the-loop oversight.

Processing over \$80 billion annually across more than 100 licences and regulatory jurisdictions globally, TransferMate own the largest non-bank licensing footprint on the planet. And, at that scale, their compliance needs to work consistently and accurately everywhere.

Alex Clements, Global Head of AML, CFT and Sanctions, describes how the goal has always been “using compliance as a competitive advantage” – keeping the bad actors out without burdening good customers with heavy-handed controls.

The challenge they encountered was doing that at scale; their analysts were spending 30 to 40 minutes per activity on manual interpretation of unstructured data, with quality varying across jurisdictions.

Following the global rollout of [NDA Client] AI agents across their KYB and compliance workflows, deep dive analysis is down from 40 minutes to as little as two minutes in some cases, and quality approval rates improved from 60% to 80% within the first two weeks of live production as the system learned continuously from senior analyst feedback.

For Alex, the confidence runs deeper than the numbers: *"The level of detail in [NDA Client]'s AI governance framework gives me confidence that we can demonstrate robust controls during audits and regulatory inspections relating to AI use."*

As he put it, *"We don't just use AI to go faster; we use it to be more certain."*

Watch the full testimonial: [LINK](#) | Read the full story: [LINK](#)

Upcoming Events

[NDA Client] is sponsoring the 6th Financial Innovation Forum – Payments & RegTech on 17 September at the Montcalm Hotel, Mayfair, London.

[X] will be on the panel discussing AI agents in financial crime – real-time scams defence, investigations, and governance – alongside senior financial crime leaders from Monzo, Revolut, Wise, Bank of China, and CEX.IO.

Register here: [link] – 10% discount available, contact info@qubevents.com to claim

[PRODUCT UPDATE PLACEHOLDER]

Discover how regulated teams deploy AI safely, transparently and in line with regulatory expectations. Try a demo today.

Book a Demo [CTA BUTTON]

Thanks for reading the July brief. At [NDA Client], we're committed to making risk and compliance operations faster, smarter and more reliable.

 Got questions or want to see a use case in action? Just hit reply.

Cheers,

The [NDA Client] Team
AI Agents for Fincrim