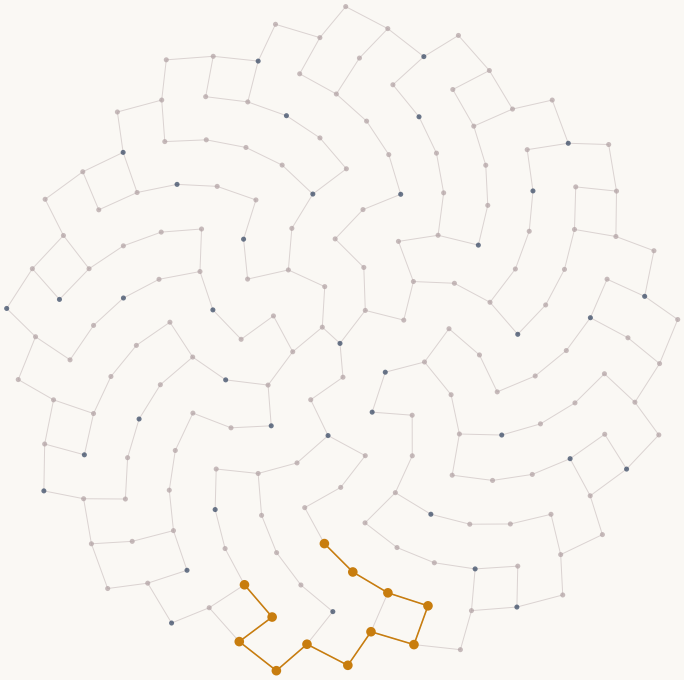

Europe's AML Coordination Problem Has a Platform Now

The EU's upgraded FIU.net enables cross-border financial intelligence sharing at speed-but banks must rethink where gaps remain visible to regulators.

By Sayari Analyst Team . Published November 2024 . sayari.com

FINANCIAL CRIME / AML

Europe's AML Coordination Problem Has a Platform Now

By Sayari Analyst Team · Published November 2024

The EU's upgraded FIU.net enables cross-border financial intelligence sharing at speed-but banks must rethink where gaps remain visible to regulators.

For decades, European financial intelligence units operated as silos. When a bank in Frankfurt reported a suspicious transaction, the FIU in Germany had it. When the same transaction's destination account sat in Amsterdam, the Dutch FIU didn't see the connection until someone manually escalated it-if at all. The money had already moved. This fragmentation was not accidental. It reflected the complexity of coordinating 27 sovereign nations with different regulatory frameworks, different disclosure rules, and different reporting timelines. Quarterly reviews became the default. By the time one FIU saw what another FIU had found, weeks or months had passed. Adversaries don't wait for quarterly reviews. That structural problem defined European AML enforcement for two decades. It also defined European compliance risk: a bank's transaction monitoring system could catch suspicious activity in one jurisdiction while missing the cross-border pattern that would have been obvious to a regulator with a unified view. The EU recognized this gap and built infrastructure to close it.

The FIU.net Goes Live

In February 2025, the next-generation FIU.net went live. For the first time, all 30 European FIUs (plus Europol, Norway, Iceland, and Liechtenstein) gained real-time access to suspicious transaction reports filed across member states. The platform created three new capabilities: cross-border reporting that automatically distributes STRs to counterpart FIUs, cross-border disseminations for FIUs to share intelligence findings, and a "Ma³tch" function allowing pseudonymous searches against shared datasets. The system is not yet fully unified, but it is no longer an archipelago of disconnected databases. This upgrade matters because it shifts the regulatory baseline. What was previously invisible to the European system is now visible. What regulators can now see, they will expect banks to see as well. That expectation will arrive in two forms: implicit, through enforcement actions on banks that miss what the FIU.net catches, and explicit, through new guidance from the EU's Anti-Money Laundering Authority, established in 2024.

What Banks Must Reconsider

The implication for banks is blunt: compliance programs built around single-jurisdiction risk assessment are incomplete. A vendor may pass German onboarding reviews and Polish sanctions screening while appearing in a Belgian FIU report for suspicious activity detected weeks earlier. Traditional vendor management assumes each jurisdiction's compliance check is independent. The FIU.net era assumes they are connected. A bank that has cleared a vendor through its home-country FIU may discover too late that a counterpart FIU has flagged that vendor in suspicious activity reports that were shared across the network in real time. The FATF (Financial Action Task Force) made this point forcefully in its 2024 mutual evaluation reports on EU member states. European financial intelligence sharing was fragmented. Competent authorities often lacked visibility into cross-border patterns. The same deficiency appeared repeatedly across mutual evaluation follow-ups. The FIU.net was the answer. For compliance officers, this creates a new operational challenge. Your AML programs may satisfy your national regulator's requirements. They may not satisfy what the broader European regulatory system now knows. A vendor relationship that was cleared by your home-country FIU may be contraindicated by intelligence shared by a counterpart FIU. Your current vendor lifecycle does not account for this-most banks refresh vendor reviews annually. The FIU.net updates in real time.

The AMLA Enforcement Shift

The AMLA (Authority for Anti-Money Laundering and Countering the Financing of Terrorism), created in 2024 and set to assume stewardship of the FIU.net by July 2027, will drive this expectation down. The AMLA's mandate is to ensure consistent application of AML/CFT rules across member states. It will do that by studying enforcement decisions, FIU referrals, and common gaps. The FIU.net intelligence will inform all of it. Banks that do not evolve their programs to account for cross-border intelligence patterns will face higher audit risk and potential enforcement action for failing to detect what regulators could see through the unified platform. The compliance program implication is this: you need visibility not just into your direct relationships, but into the intelligence that regulators now share about those relationships across borders. That visibility is not available from point-in-time vendor screening. It requires continuous monitoring against data that changes-adverse information discovered in one FIU system, immediately relevant to all of them. A vendor flagged in suspicious activity reports from one jurisdiction is now visible to FIUs across the EU network, sometimes before banks receive formal notice.

The Regulatory Visibility Gap

The commercial world is not yet as connected as the regulatory world now is. Most banks still integrate data from fragmented sources: their own systems, their home-country FIU (if they have access), and third-party vendor databases. The FIU.net has created asymmetry. European regulators now see connections that banks do not. This regulatory visibility advantage will not last-it will eventually become a compliance expectation applied to banks that fail to keep pace. The AMLA has already begun coordinating enforcement strategy across member states. Banks that operate in multiple European jurisdictions will find themselves subject to harmonized expectations about what they should have seen and what action they should have taken. A vendor that appears in FIU.net data and is flagged by any member state's FIU creates liability for any bank using that vendor, regardless of whether that bank's home-country regulator has yet taken action. Connect with Sayari to map your third-party networks with the same visibility regulators now have. Sayari's platform connects data across jurisdictions the way the FIU.net connects financial intelligence-revealing ownership structures, beneficial owners, and risk patterns that point-in-time screening misses. This visibility is no longer optional in the European regulatory environment. Explore Financial Crime to see how Sayari helps compliance teams stay ahead of evolving regulatory baselines, and request a demo to see your vendor network the way European regulators now do.

Please visit sayari.com to learn more.

This blog is for informational purposes and isn't intended to be legal advice.