



TOPICS:
AML/CFT

SOURCE

European Banking Authority

EBA: Supervisors Should Learn from Recent Cases to Prevent Financial Crime in Crypto Firms

- This EBA report analyses **the evolving landscape of money laundering (ML) and terrorist financing (TF) risks in the EU's crypto-asset sector**, particularly in the context of the implementation of Regulation (EU) 2023/1114 (MiCA) and the EU's enhanced AML/CFT legislative framework. It draws on supervisory data and case studies to assess how crypto-asset service providers (CASPs) have attempted to circumvent regulation, and how the new framework addresses these risks.
- The report identifies **key strategies used by CASPs to evade AML/CFT oversight**, including operating without authorisation, exploiting regulatory fragmentation through 'forum shopping', abusing reverse solicitation exemptions, and engaging in opaque ownership or governance arrangements. Deficiencies in internal AML/CFT frameworks, such as poor customer due diligence, inadequate transaction monitoring, and weak outsourcing arrangements, were also prevalent. Additionally, the use of multi-entity structures, particularly with ties to high-risk or unregulated jurisdictions, further compounded supervisory challenges.
- In response, the new framework under MiCA introduces an **EU-wide authorisation and passporting regime**, enhanced governance and transparency standards, and stricter beneficial ownership and fitness requirements. CASPs must now adhere to harmonised AML/CFT obligations, with regulators empowered to take dissuasive enforcement actions, including licence revocation. The transition period (until July 2026) poses residual risks, especially from legacy entities and inconsistent national practices.
- The report emphasises that **effective implementation** is critical. National competent authorities (NCAs) are urged to apply robust scrutiny during the authorisation process, particularly for entities with historical compliance failings. Ongoing supervisory cooperation, both within the EU and with third countries, is essential to mitigate cross-border risks and prevent regulatory arbitrage. The use of technology, supervisory intelligence sharing, and market surveillance tools is also encouraged to monitor emerging threats, such as DeFi-linked activities and stablecoin misuse.

FOLLOW US!

