Seqlense

Cécile Henry
General Manager, CLR & Co-Founder

Crypto-Asset Services
EBA Report on ML/TF risks

In October 2025, the European Banking Authority (EBA) issued a *Report on Tackling ML/TF Risks in Crypto-Asset Services*. This report provides a structured **review of money laundering and terrorist financing (ML/TF) vulnerabilities in the crypto-asset sector** and guidance to strengthen European supervisory practices under MiCA.

The crypto-asset sector is known to be fast-growing and dynamic from a technological point of view, but it is also vulnerable to ML/FT misuse. MiCA (Regulation EU 2023/1114) and the new AML package (AMLR, AMLD6, AMLAR) introduce safeguards with harmonised authorisation, governance, and transparency. The EBA reviewed how firms evaded rules before MiCA and the role of supervisory authorities in fixing these weaknesses. The key risks observed are related to **unauthorised operations, forum shopping, weak AML controls, opaque ownership, and complex group structures**.

The report aims to:

- Identify **key ML/TF risks** related to crypto-asset services.
- Assess **supervisory practices** and their level of maturity across EU Member States.
- Promote **consistent, risk-based supervision** of CASPs across the Union.
- Provide **recommendations** to prepare national authorities for AMLA's direct supervision of certain high-risk CASPs.

Identified ML/TF evasion Strategies

The EBA report highlights the following identified ML/TF strategies:

Operating without approval

Some firms serviced EU clients without the required registration or authorisation. The common tactics observed consist of working from outside the EU or relying on delayed

MiCA grandfathering periods. In front of these elements, supervisors imposed sanctions and withdrawals of authorisation.

Forum shopping
It has been observed that some entities chose EU jurisdictions with lighter oversight. They withdrew when scrutiny increased. This regulatory arbitrage undermined AML standards, but MiCA's harmonised regime aims to end this practice.

Misuse of reverse solicitation
Some third-country CASPs falsely claimed that European clients approached them through reverse solicitation. The new MiCA framework strictly defines and limits this exemption.

Weak AML/CTF compliance
Frequent failures have been observed in relation to **missing KYC/EDD**, **poor sanctions screening**, or uninformed compliance staff. Outsourcing to third countries often lacked European oversight. Deficiencies included **missing Travel Rule implementation** and **poor reporting**. A specific case highlighted the use of DeFi as a conduit for illicit flows, where exchanges acted as unregulated on/off-ramps.

Unclear beneficial ownership
Complex and opaque structures made it challenging to trace ultimate control. Discrepancies existed between jurisdictions, often intentionally to hide ownership.

Multi-entity high-risk structures
Entities used linkages such as subsidiaries, partnerships, or stakes in financial firms to avoid scrutiny. Some stablecoin issuers exploited cross-border group models such as "one-leg-out" issuances to arbitrage MiCA rules.

Safeguards and supervisory priorities

The main recommendations include, among others, **strengthening the technical and human capacities of AML/CFT supervisors** and e**stablishing a common approach to risk** at the European level, based on shared typologies. The EBA promotes a unified, risk-based supervisory framework to identify and mitigate ML/TF threats.

Supervisors face significant difficulties in obtaining information and coordinating across jurisdictions. Therefore, **cross-border cooperation** and **information exchange** between national authorities are encouraged.

Greater use of blockchain analytics, transaction monitoring, and digital supervisory tools is essential. Among the recommendations, developing digital supervision tools, including transaction traceability and on-chain monitoring capabilities, is expected.

Supervision should also be proportionate to each CASP's size, complexity, and risk exposure. Strengthening the supervision of new players, such as **centralised DeFi service providers, non-custodial wallet providers, and NFT intermediaries, where applicable, is also a recommendation** highlighted in the EBA report. Privacy-enhancing tools, peer-to-peer transfers, DeFi intermediaries, and NFT-related services also pose emerging risks.

Preparing for the transition to AMLA supervision, particularly through common reporting standards and harmonised risk indicators, is another expected significant step. The report encourages aligning national supervision ahead of the AMLA's direct oversight of high-risk CASPs.

The conclusion of this report emphasises that the MiCA-AML package represents the EU's **first holistic crypto regulatory system**. Its success depends on consistent supervisory implementation, strong cross-border coordination, and proactive risk assessments. AMLA will assume EBA's AML/CTF role from the end of 2025, ensuring convergence and continued monitoring of crypto markets.

EBA's key points in DeFi

DeFi is not fully outside the AML/CFT scope

According to this report from the EBA, **DeFi is not fully outside the AML/CFT scope**. The EBA warns that DeFi cannot be automatically considered as unregulated. If a person or entity exerts control or influence over a protocol or offers access/interface services (for example, front-ends, custodial wallets, aggregators, staking-as-a-service), they qualify as a CASP under MiCA and are therefore subject to AML/CFT obligations.

Crypto-Asset Services – EBA Report on ML/TF risks

Cécile Henry
General Manager, CLR & Co-Founder

In point 1.4 of the EBA report, the following is enounced:
Finally, despite not being a regulated activity, risks also stem from unmonitored entry and exit activity with DeFi platforms(16). When CASPs interact with DeFi services without recognising or mitigating the associated heightened ML/TF risks, they provide channels that allow criminal actors to obfuscate transactions, bypass supervised intermediaries, and obfuscate traceability. This creates layering opportunities that further complicate detection and enforcement.

The report also stresses the importance of identifying the "mind and management" behind DeFi projects, even if DAOs or governance tokens are used to disguise centralised control.

According to this report, a regulated CASP providing access to DeFi, such as routing clients to liquidity pools or staking protocols, cannot ignore AML/CFT obligations on the grounds that the underlying protocol is decentralised.

Risk-based approach

The EBA report repeatedly makes references to DeFi as a significant and emerging ML/TF risk. CASPs acting as entry or exit points to DeFi protocols are often unaware or dismissive of risk exposure. The report provides some examples of cases where illicit flows were found.

DeFi-related risks are included among the new and emerging ML/TF typologies, such as, among others:

- Obfuscation of transaction trails through smart contract routing,
- Use of bridges and cross-chain swaps,
- Liquidity pool manipulation and self-laundering,
- DAO governance tokens used to control multiple projects.

Supervisors are warned that DeFi can create "layering opportunities" that obscure traceability, complicating enforcement. The EBA urges authorities to develop typology-based red flags for DeFi interactions and to include them in risk assessments of supervised entities. Supervisors are encouraged to adopt tools to trace and visualise transactions, including DeFi protocols, mixing services, and decentralised exchanges (DEXs). The report from EBA highlights the need for on-chain monitoring that covers interaction with smart contracts, cross-chain swaps, and DeFi token exposure.

The EBA urges authorities to **develop typology-based red flags** for DeFi interactions and to include them in risk assessments of supervised entities.

DeFi intermediaries and hybrid structures

The EBA report explicitly mentions **"intermediaries operating within DeFi structures"** as a **supervisory blind spot**.
Some CASPs act as **gateways** to DeFi by offering:

- **custodial staking**,
- **yield products**, or
- **wrapped/derivative tokens** linked to DeFi yields.

These business models often rely on **third-party node operators, validators, or protocols** not subject to AML/CFT oversight.

CASPs remain **fully responsible** for AML/CFT controls, even if the operational risk lies with a DeFi counterparty. Any **outsourcing or delegation** (e.g., to a validator, protocol, or liquidity provider) must comply with EU outsourcing standards — contractual clauses, audit rights, clear responsibilities, and exit plans.

Sources :
https://www.eba.europa.eu/legacy/regulation-and-policy/regulatory-activities/anti-money-laundering-and-countering-financing-1

Seqlense

Cécile Henry
General Manager, CLR & Co-Founder

Services liés aux crypto-actifs
Rapport de l'EBA sur les risques liés au blanchiment de capitaux et au financement du terrorisme

En octobre 2025, l'Autorité bancaire européenne (*European Banking Authority* ou EBA) a publié un rapport sur la lutte contre les risques liés au blanchiment de capitaux et au financement du terrorisme dans les services liés aux crypto-actifs *(Report on Tackling ML/TF Risks in Crypto-Asset Services)*. Ce rapport fournit une **analyse structurée des vulnérabilités en matière de blanchiment de capitaux et de financement du terrorisme (BC/FT) dans le secteur des crypto-actifs**, ainsi que des orientations visant à renforcer les pratiques de surveillance européennes dans le cadre du règlement MiCA.

Le secteur des crypto-actifs est connu pour être en pleine croissance et dynamique d'un point de vue technologique, mais il est également vulnérable aux abus en matière de ML/FT. Le règlement MiCA (règlement UE 2023/1114) et le nouveau paquet AML (AMLR, AMLD6, AMLAR) introduisent des mesures de protection avec une autorisation, une gouvernance et une transparence harmonisées. L'EBA a examiné la manière dont les entreprises contournaient les règles avant MiCA et le rôle des autorités de surveillance dans la correction de ces faiblesses. Les principaux risques observés sont liés aux **opérations non autorisées, au forum shopping, à la faiblesse des contrôles de lutte contre le blanchiment d'argent (*Anti Money Laundering* ou AML), à l'opacité de la propriété et à la complexité des structures** des groupes.

Le rapport vise à :

- Identifier les **principaux risques de ML/TF** liés aux services de crypto-actifs.
- Évaluer les **pratiques de surveillance** et leur niveau de maturité dans les États membres de l'UE.
- Promouvoir une **surveillance cohérente et fondée sur les risques** des PSCA/CASP dans toute l'Union.
- Formuler des **recommandations** afin de préparer les autorités nationales à la surveillance directe par l'AMLA de certains PSCA/CASP à haut risque.

Cécile Henry
General Manager, CLR & Co-Founder

Stratégies identifiées de contournement des règles en matière de ML/TF

Le rapport de l'EBA met en évidence les stratégies suivantes identifiées en matière de ML/TF :

Exercice sans agrément
Certaines entreprises fournissaient des services à des clients de l'UE sans avoir obtenu l'enregistrement ou l'agrément requis. Les tactiques courantes observées consistent à travailler depuis l'extérieur de l'UE ou à compter sur des périodes de transition sous MiCA (clause du « grand-père »). Face à ces éléments, les autorités de surveillance ont imposé des sanctions et des retraits d'autorisation.

Forum shopping
Il a été observé que certaines entités choisissaient des juridictions de l'UE où la surveillance était moins stricte. Elles se retiraient lorsque la surveillance s'intensifiait. Cet arbitrage réglementaire a sapé les normes AML, mais le régime harmonisé de MiCA vise à mettre fin à cette pratique.

Utilisation abusive de la sollicitation inversée
Certains PSCA/CASP de pays tiers ont faussement prétendu que des clients européens les avaient approchées par le biais d'une sollicitation inversée. Le nouveau cadre MiCA définit et limite strictement cette exemption.

Faible conformité AML/CTF
Des défaillances fréquentes ont été observées en matière d'**absence de KYC/EDD**, de **mauvais contrôle des sanctions** ou de personnel de conformité mal informé. L'externalisation vers des pays tiers manquait souvent de surveillance européenne. Les lacunes comprenaient l'**absence de mise en œuvre de la *Travel Rule*** et la **mauvaise qualité des rapports**. Un cas spécifique a mis en évidence l'utilisation de la DeFi comme canal pour les flux illicites, les *exchanges* agissant comme des rampes d'accès et de sortie non réglementées.

Propriétaire bénéficiaire
Des structures complexes et opaques rendaient difficile la traçabilité du contrôle ultime. Il existait des divergences entre les juridictions, souvent intentionnelles afin de dissimuler la propriété.

Structures à haut risque multi-entités
Les entités utilisaient des liens tels que des filiales, des partenariats ou des participations dans des sociétés financières pour échapper à la surveillance. Certains émetteurs de stablecoins ont exploité des modèles de groupes transfrontaliers tels que les émissions « one-leg-out » pour arbitrer les règles MiCA.

Mesures de protection et priorités en matière de surveillance

Les principales recommandations comprennent, entre autres, le **renforcement des capacités techniques et humaines des autorités de surveillance LCB/FT** et la **mise en place d'une approche commune du risque** au niveau européen, basée sur des typologies communes. L'EBA promeut un cadre de surveillance unifié et fondé sur les risques afin d'identifier et d'atténuer les menaces de blanchiment d'argent et de financement du terrorisme.

Les autorités de surveillance rencontrent des difficultés importantes pour obtenir des informations et coordonner leurs actions entre les différentes juridictions. Par conséquent, la **coopération transfrontalière** et l'**échange d'informations** entre les autorités nationales sont encouragés.

Il est essentiel de recourir davantage à l'analyse de la blockchain, à la surveillance des transactions et aux outils de surveillance numériques. Parmi les recommandations, on peut s'attendre à ce que des outils de surveillance numériques soient développés, notamment des capacités de traçabilité des transactions et de surveillance en chaîne.

La surveillance doit également être proportionnée à la taille, à la complexité et à l'exposition au risque de chaque PSCA/CASP. Le renforcement de la surveillance des nouveaux acteurs, tels que les **fournisseurs de services DeFi centralisés, les fournisseurs de portefeuilles non dépositaires et les intermédiaires NFT, le cas échéant, est également une recommandation** mise en avant dans le rapport de l'EBA. Les outils de renforcement de la confidentialité, les transferts *peer-to-peer*, les intermédiaires DeFi et les services liés aux NFT présentent également des risques émergents.

La préparation à la transition vers la supervision AMLA, notamment par le biais de normes communes de déclaration et d'indicateurs de risque harmonisés, est une autre

étape importante attendue. Le rapport encourage l'harmonisation de la supervision nationale avant la supervision directe par l'AMLA des PSCACASP à haut risque.

La conclusion de ce rapport souligne que le paquet MiCA-AML représente le **premier système réglementaire holistique de l'UE en matière de cryptomonnaies**. Son succès dépend d'une mise en œuvre cohérente de la surveillance, d'une coordination transfrontalière solide et d'évaluations proactives des risques. L'AMLA assumera le rôle de l'EBA en matière de LBC/FT à partir de la fin de 2025, garantissant la convergence et la surveillance continue des marchés des cryptomonnaies.

Points clés de l'EBA concernant la DeFi

La DeFi n'est pas totalement exclue du champ d'application de la lutte contre le blanchiment d'argent et le financement du terrorisme

Selon ce rapport de l'EBA, **la DeFi n'est pas totalement exclue du champ d'application de la lutte contre le blanchiment d'argent et le financement du terrorisme**. L'EBA avertit que la DeFi ne peut pas être automatiquement considérée comme non réglementée. Si une personne ou une entité exerce un contrôle ou une influence sur un protocole ou offre des services d'accès/d'interface (par exemple, des interfaces utilisateur, des portefeuilles de conservation, des agrégateurs, des services de staking), elle est considérée comme un PSCA/CASP au sens de MiCA et est donc soumise aux obligations AML/CFT.

Au point 1.4 du rapport de l'EBA, il est énoncé ce qui suit :
Enfin, bien qu'il ne s'agisse pas d'une activité réglementée, des risques découlent également des activités d'entrée et de sortie non surveillées sur les plateformes DeFi(16). Lorsque les CASP interagissent avec les services DeFi sans reconnaître ni atténuer les risques accrus de ML/TF qui y sont associés, ils fournissent des canaux qui permettent aux acteurs criminels de dissimuler des transactions, de contourner les intermédiaires supervisés et de brouiller la traçabilité. Cela crée des opportunités de stratification qui compliquent encore davantage la détection et l'application de la loi.

(Finally, despite not being a regulated activity, risks also stem from unmonitored entry and exit activity with DeFi platforms(16). When CASPs interact with DeFi services without recognising or mitigating the associated heightened ML/TF risks, they provide channels that allow criminal actors to obfuscate transactions, bypass supervised intermediaries, and obfuscate traceability. This creates layering opportunities that further complicate detection and enforcement.)

Le rapport souligne également l'importance d'identifier l'esprit et la gestion derrière les projets DeFi, même si des DAO ou des jetons de gouvernance sont utilisés pour dissimuler un contrôle centralisé.

Selon ce rapport, un PSCA/CASP réglementé fournissant un accès à la DeFi, par exemple en acheminant des clients vers des pools de liquidité ou des protocoles de staking, ne peut ignorer ses obligations en matière de LBC/FT au motif que le protocole sous-jacent est décentralisé.

Approche fondée sur les risques

Le rapport de l'EBA fait référence à plusieurs reprises à la DeFi comme un risque important et émergent en matière de ML/TF. Les PSCA/CASP qui servent de points d'entrée ou de sortie aux protocoles DeFi ignorent souvent leur exposition au risque ou la minimisent. Le rapport fournit quelques exemples de cas où des flux illicites ont été détectés.

Les risques liés à la DeFi font partie des typologies nouvelles et émergentes de ML/TF, telles que, entre autres :
· L'obscurcissement des traces de transactions par le routage de contrats intelligents,
· L'utilisation de ponts et d'échanges inter-chaînes,
· La manipulation des pools de liquidités et l'auto-blanchiment,
· Les jetons de gouvernance DAO utilisés pour contrôler plusieurs projets.

Les superviseurs sont avertis que la DeFi peut créer des « opportunités de stratification » qui obscurcissent la traçabilité, compliquant ainsi l'application de la loi. L'EBA exhorte les autorités à élaborer des signaux d'alerte basés sur la typologie pour les interactions DeFi et à les inclure dans les évaluations des risques des entités supervisées. Les autorités de surveillance sont encouragées à adopter des outils permettant de tracer et de visualiser les transactions, y compris les protocoles DeFi, les services de mixage et les bourses décentralisées (DEX). Le rapport de l'EBA souligne la nécessité d'une surveillance en chaîne qui couvre les interactions avec les contrats intelligents, les échanges inter-chaînes et l'exposition aux jetons DeFi.

L'EBA exhorte les autorités à **développer des signaux d'alerte basés sur la typologie** pour les interactions DeFi et à les inclure dans les évaluations des risques des entités supervisées.

Intermédiaires DeFi et structures hybrides

Le rapport de l'EBA mentionne explicitement les **intermédiaires opérant au sein de structures DeFi** comme un **angle mort de la surveillance**.
Certains PSCA/CASP agissent comme des **passerelles** vers la DeFi en proposant :

- **du *custodial staking***,
- **des produits à rendement (*yield products*)**, ou
- **des *wrapped/derivative tokens*** liés aux rendements DeFi.

Ces modèles commerciaux s'appuient souvent sur **des opérateurs de nœuds (*node operators*), des validateurs ou des protocoles tiers** qui ne sont pas soumis à la surveillance LCB/FT.

Les PSCA/CASP restent **entièrement responsables** des contrôles LCB/FT, même si le risque opérationnel incombe à une contrepartie DeFi. Toute **externalisation ou délégation** (par exemple à un validateur, un protocole ou un fournisseur de liquidité) doit être conforme aux normes européennes en matière d'externalisation : clauses contractuelles, droits d'audit, responsabilités claires et plans de sortie.

Sources :
https://www.eba.europa.eu/legacy/regulation-and-policy/regulatory-activities/anti-money-laundering-and-countering-financing-1