REPORT ON TACKLING ML/TF RISKS IN CRYPTO-ASSET SERVICES THROUGH SUPERVISION

LESSONS LEARNED FROM RECENT CASES

EBA/REP/2025/28 OCTOBER 2025

Contents

Executive summary **3**
Introduction **4**
Methodology 5
Legal basis 6
1. Certain crypto-asset businesses sought to evade national AML/CFT supervision, undermining the integrity of the EU financial system **7**
1.1 Entities operating without regulatory approval 7
1.2 'Forum shopping' 8
1.3 Exploitation of the reverse solicitation exemption 9
1.4 Weaknesses in AML/CFT compliance and risk management 10
1.5 Unclear beneficial ownership and governance structures 12
1.6 Multi-entity arrangements with high-risk entities 13
2. The new framework introduces safeguards, but competent authorities should pay attention to specific ML/TF factors to ensure its effective implementation **17**
2.1 An EU-wide authorisation and passporting regime with enhanced supervisory powers 17
Definition of exit strategies for unauthorised CASPs post-grandfathering 18
Monitoring the perimeter for unauthorised activities 18
Ensuring the adequate application of the MiCA authorisation procedure on entities with legacy AML/CFT issues 19
2.2 Integration into AML/CFT framework and enhanced AML/CFT obligations 20
Keeping abreast of developments in controls and ML/TF risks 20
2.3 Heightened transparency, governance and beneficial ownership requirements 21
Overseeing changes in ownership structure and entity (in)dependency 22
Ensuring adequate and timely reassessment of fitness and propriety 22
Monitoring linked entities in AML/CFT supervision 23
2.4 Supervisory cooperation and public transparency 24
Focusing on effective cooperation and information-sharing among authorities 24
Ensuring the effectiveness of the Central Contact Point role 25
3. Conclusion **27**

Executive summary

The crypto-asset sector is technologically dynamic and growing rapidly. It is also vulnerable to being used for money laundering and terrorist financing (ML/TF) purposes. This is why certain crypto-asset activities were brought within the scope of the EU's anti-money laundering and countering the financing of terrorism (AML/CFT) regime in 2018. Subsequently, on 31 December 2024, Regulation (EU) 2023/1114 (MiCA) introduced a unified rulebook for crypto-asset issuance, trading and service provision. At the same time, the EU's AML/CFT legislative framework was extended to include a broader range of crypto-asset activities. As a result, the EU now has a more comprehensive regulatory and supervisory framework for tackling ML/TF risk in this sector.

This report summarises the lessons learned from actions taken by AML/CFT competent authorities (CAs) and the European Banking Authority (EBA) regarding the identification and management of ML/TF risks associated with crypto-asset businesses, both before and immediately after the implementation of the new regulatory framework. It examines strategies some entities have used to circumvent AML/CFT supervision, including unauthorised operations, forum shopping across Member States, improper use of the reverse solicitation exemption, weak AML/CFT frameworks, opaque ownership and governance structures, and multi-entity arrangements involving high-risk counterparties.

The report also highlights the safeguards introduced by MiCA and the AML/CFT regime to address ML/TF risks and identifies measures to ensure their effective application. Together, MiCA and the strengthened AML/CFT rules establish safeguards, including a harmonised authorisation and passporting regime, stricter governance requirements, transparency in beneficial ownership, and comprehensive integration of AML/CFT obligations. Effective implementation will depend on vigilant monitoring of unauthorised activities, thorough assessment of legacy AML/CFT issues, continuous risk identification, and supervision of linked entities. Equally important are strong cross-border cooperation, information-sharing among CAs, and public transparency to prevent regulatory gaps from being exploited.

By consolidating these findings, this report aims to support the effective implementation of the new MiCA and enhanced AML/CFT frameworks, while promoting a robust and forward-looking approach to tackling financial crime risk in the sector.

Introduction

The blockchain technology underpinning crypto-asset services provision offers opportunities in the fight against financial crime. These opportunities include, for example:

- **Enhanced traceability**, because most blockchain transactions – although not always connected to verified identities – are recorded on a public ledger, which means that they are immutable, timestamped, and accessible to anyone in real time.
- **Transaction monitoring**, as it facilitates the identification of some patterns of transactions and helps trace the origin and destination of assets across multiple transactions.
- **Compliance**, because smart contracts can be programmed to automatically enforce certain regulatory requirements (e.g. blocking transactions from sanctioned addresses).
- **Data protection**, because privacy-preserving blockchain-based identity solutions can help strike a balance between privacy and compliance, allowing verification of the customer's identity without sharing personal data.

At the same time, crypto-assets and crypto-asset businesses are susceptible to being misused for ML/TF purposes. In recent years, several crypto-asset firms have been subject to high-profile enforcement actions, such as orders to cease operations and significant fines for failure to comply with applicable AML/CFT and sanctions obligations. Some firms have also been involved in judicial proceedings which have resulted, in some cases, in criminal penalties.

Furthermore, the cross-border nature of crypto businesses creates challenges from a supervisory and law enforcement perspective. The global reach of the sector's services and activities can make it challenging for CAs to obtain a comprehensive view of an institution's ML/TF risk exposure. The fragmented approach to regulating and supervising crypto-asset services that prevailed in the EU prior to the implementation of MiCA created gaps that some businesses exploited. Its impact is still visible today, as firms with legacy compliance issues continue to operate in the EU.

To address these challenges, the EU brought custodian wallet providers, and providers engaged in exchange services between virtual and fiat currencies, within the scope of Directive (EU) 2015/849 (AMLD5)([1]). In December 2024, a more comprehensive regime for the regulation and supervision of crypto-asset businesses – issuance, trading, and service provision – came into force([2]) with MiCA. At the same time, Regulation (EU) 2023/1113 introduced amendments to AMLD5 to extend it to a wider range of crypto-asset service providers (CASPs)([3]). The AML/CFT framework was also enhanced with

[1] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU.

[2] The regime for the issuance of asset-referenced tokens (ARTs) and e-money tokens (EMTs) became applicable earlier, in June 2024. In addition, under MiCA's transitional arrangements, some service providers remain subject to national supervision for a limited period before full transfer of responsibilities to EU-level oversight.

[3] To ensure clarity, this document will refer to all crypto-asset businesses covered by MiCA as CASPs, and those that existed before its implementation as VASPs.

the introduction of specific references to crypto-assets and their supervision in Regulation (EU) 2024/1624 (AMLR)([4]), Directive (EU) 2024/1640 (AMLD6)([5]), and Regulation (EU) 2024/1620 (AMLAR)([6]). The EBA and European Securities and Markets Authority (ESMA) issued regulatory instruments([7]) to complement this regime. The focus now shifts to the effective implementation of the new regime.

The EBA has played a key role in strengthening the AML/CFT regulatory and supervisory framework for crypto-assets in the EU since the beginning. Through continuous engagement and cooperation with EU national supervisors, European Supervisory Authorities (ESAs) and third country authorities, the EBA has gathered critical insights into the operation and risks of crypto-assets businesses, both before and after the implementation of MiCA. This has allowed the EBA to identify significant AML/CFT vulnerabilities across the sector and to provide targeted guidance to improve compliance and oversight. Additionally, the EBA's collection and analysis of data via EuReCA([8]), the EBA's central AML/CFT database, has enhanced understanding of ML/TF risks linked to crypto-assets.

This report summarises the EBA's findings. It aims to inform emerging supervisory approaches to the authorisation and supervision of CASPs and to strengthen AML/CFT oversight mechanisms. It describes the ML/TF risks posed by CASPs' strategies that have allowed them to sidestep national AML/CFT supervision and its impact on the new regulatory regime. It also highlights the safeguards introduced by MiCA and the new AML/CFT regulatory regime to address those ML/TF risks, and identifies key AML/CFT considerations to CAs for the effective application of the new EU framework.

Responsibilities under MiCA are divided between the ESMA and the EBA. The ESMA is the primary authority for the regulation and supervision of CASPs under MiCA, while the EBA is the main authority for issuers of ARTs and EMTs. The EBA is also responsible for AML/CFT, and contributes to broader coordination across CAs until these powers are transferred to the Anti-Money Laundering Authority (AMLA) at the end of 2025. After 2025, the ESMA and the EBA will remain responsible for tackling financial crime through their respective MiCA mandates.

Methodology

This report summarises the insights gathered from CAs' work on tackling ML/TF risks in the sector before and immediately after the implementation of the new regulatory regimes that took effect in December 2024.

[4] Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (OJ L, 2024/1624, 19.6.2024, ELI: http://data.europa.eu/eli/reg/2024/1624/oj).

[5] Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on the mechanisms to be put in place by MSs for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive(EU) 2019/1937, and amending and repealing Directive (EU) 2015/849 (OJ L, 2024/1640, 19.6.2024, ELI: http://data.europa.eu/eli/dir/2024/1640/oj).

[6] Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010 (OJ L, 2024/1620, 19.6.2024, ELI: http://data.europa.eu/eli/reg/2024/1620/oj).

[7] See 'Preventing money laundering and terrorism financing in the EU's crypto-assets sector'.

[8] See Factsheet on 'EuReCA, the EBA's AML/CFT database'.

It draws on qualitative data collected by the EBA from the following sources of information:

- Information provided by EU supervisors responsible for the registration, licensing, authorisation([9]) and supervision of Virtual Asset Service Providers (VASPs)/CASPs and issuers of crypto-assets, before and after the implementation of MiCA, in response to specific information requests and in the context of the ESAs' subgroups and supervision workshops.
- Information provided by third country supervisors responsible for the AML/CFT supervision of issuers of crypto-assets and VASPs/CASPs providing their services in EU Member States (MSs).
- Information obtained via evaluations performed or contributed to by the EBA (e.g. peer reviews).
- Information from the EBA's AML/CFT Database, EuReCA.
- 2025 Opinion of the EBA on ML/TF risks affecting the EU's financial sector([10]).
- Letters received from market players on the challenges faced by VASPs/CASPs and issuers of crypto-assets.
- Desk-based research and market monitoring by EBA staff in the context of the EBA's statutory duties set out in Regulation (EU) No 1093/2010 (EBA Founding Regulation)([11]).

Legal basis

Under Article 1(5) of the EBA Founding Regulation, the EBA has a general objective of ensuring the integrity of financial markets and preventing the use of the financial system for the purposes of ML/TF. In the context of Article 8(1)(1), the EBA must do so by promoting consistent, efficient and effective application of legislative acts with regards to the prevention of the use of the financial system for the purposes of ML/TF.

For that purpose, Article 9a gives the EBA a leading, coordinating and monitoring role in promoting integrity, transparency and security in the financial system. Article 31(1) of the EBA Regulation provides for the EBA having a coordination role between CAs where adverse developments could potentially jeopardise the orderly functioning and integrity of financial markets or the stability of the financial system in the Union. In addition, Article 31(2), point (ea) of that Regulation requires the EBA to take appropriate measures to coordinate actions undertaken by relevant CAs with a view to facilitating the entry into the market of actors or products relying on technological innovation.

[9] This report distinguishes between 'licensing' and 'registration' – used in the context of pre-December 2024 market entry requirements – and 'authorisation' under the MiCA framework.

[10] See EBA/Op/2025/10.

[11] Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC.

1. Certain crypto-asset businesses sought to evade national AML/CFT supervision, undermining the integrity of the EU financial system

Since the introduction of AML/CFT obligations for certain VASPs under EU law in 2018, and after the implementation of MiCA and the enhanced AML/CFT regime in December 2024, supervisory findings point to attempts by some entities to circumvent regulatory requirements and AML/CFT oversight. There is a risk that such attempts may continue under the new regime, with a significant and adverse impact on the integrity of the EU's financial system. This section explores those identified strategies and risks, both before and after December 2024, noting that their impact will persist under the new regulatory framework regardless, if overlooked by supervisors.

1.1 Entities operating without regulatory approval

Prior to the application of MiCA, VASPs offering services within the EU were required under AMLD5 and applicable domestic AML/CFT regimes to register or obtain a licence in each MS in which they operated. In addition, before 2025 some 'issuers' were already obliged entities under the AMLD as credit institutions and e-money institutions. To the extent provided for under each of those regimes, these entities were subject to supervisory oversight, and had to comply with specific AML/CFT obligations. Some sought to circumvent local licensing or registration requirements, and therefore supervision. CAs have identified two main strategies employed to operate without regulatory approval:

- Entities providing services in a MS from another EU jurisdiction without the requisite permission to do so by the host supervisor, where applicable.
- Entities providing services in a MS from a third country that has not yet implemented a robust regulatory and supervisory framework for VASPs and that, consequently, has not yet taken the steps necessary to ensure adequate AML/CFT compliance.

In response, CAs took various supervisory measures, ranging from public warnings and administrative fines to orders to cease operations, particularly under MiCA. In MSs where such conduct is a criminal offence, supervisors reported these entities to the relevant judicial authorities.

CAs noted that, when these entities later submitted their interest or applied for MiCA authorisations, their files were often incomplete or included AML/CFT programmes that did not meet the expected EU standards.

Use Case 1. The same entity was found to be providing services from a third country in four Member States without registration or licensing at different periods between 2019 and 2024. All

CAs imposed measures, including several warnings which had little effect and, finally, orders to cease operations. When the same entity showed interest in applying for MiCA authorisation in other Member States, issues were identified in its shareholder structure and governance.

Furthermore, Article 143 of MiCA provides for a transitional arrangement (commonly known as 'grandfathering'), allowing CASPs that provided their services in accordance with the applicable law to continue operating under it until 1 July 2026 or until it is granted or refused MiCA authorisation, whichever is sooner. When this period has ended([12]), entities whose applications for authorisation have been unsuccessful will no longer be allowed to operate in the EU. At the same time, emerging evidence suggests that there may be a risk that entities which were previously licensed in a Member State and have not met the authorisation conditions under MiCA but are appealing their case may continue to operate in the EU in the intervening time.

Use Case 2. A VASP already licensed in a MS submitted a MiCA application in early 2025, which was subsequently rejected due to serious AML/CFT deficiencies. Despite the official end of the transitional period, the entity continues to operate under the national VASP regime, as it has appealed the decision. The national framework of the jurisdiction allows the entity to continue its business until a final decision is reached. The company has also submitted a MiCA application in another MS, indicating potential forum shopping.

CASPs or issuers operating without regulatory approval pose several ML/TF risks that will continue to apply under the new regulatory regime if such practices persist. CAs may be unable to supervise these entities effectively, as they may lack proactive strategies to detect unregulated activities at an early stage. This makes it difficult to ensure adherence to legal and regulatory obligations, leaving customers and the wider financial system exposed to financial crime.

In addition, the operation of unauthorised businesses in the EU creates an uneven playing field. Authorised providers dedicate substantial resources to meeting stringent AML/CFT obligations and supervisory expectations. By contrast, unauthorised entities avoid these requirements and often operate with significantly lower (or no) compliance and operational costs. This not only grants them an unfair competitive advantage over regulated players but also undermines market fairness and erodes trust in the EU financial market.

1.2 'Forum shopping'

Before MiCA was adopted, some entities sought to exploit regulatory fragmentation by applying for registration or licensing in jurisdictions they perceived as having less stringent market entry and supervision requirements or approaches. When faced with CA scrutiny – such as concerns over inadequate AML/CFT controls – these entities often failed to respond to information requests, withdrew their applications and attempted to restart the same process in another MS. CAs also

[12] See List of grandfathering periods decided by Member States under MiCA.

observed that, in some cases, businesses voluntarily withdrew from the market after on-site inspections had been launched.

Use Case 3. One entity submitted applications for registration and licensing in multiple EU MSs within a short timeframe. It withdrew from jurisdictions where CAs asked questions or its application was challenged, but began operating from those MS where no such challenges were made. In one case, after receiving an order to cease operations in MS A, the entity transferred the local customers it had already onboarded to another group entity licensed in MS B. Due to the national framework of MS A([13]), this allowed the group to continue to provide services to customers in MS A, effectively circumventing local supervisory scrutiny.

In addition, information from CAs suggests that some VASPs and issuers may have sought licences under the old national regime – perceived as more permissive – specifically to benefit from longer transitional periods. In some cases, MSs actively encouraged entities to obtain a national licence before MiCA took effect to manage expected authorisation volumes.

Forum shopping by CASPs or issuers creates significant ML/TF risks, which may persist under the new regulatory framework if divergent supervisory approaches continue to apply across jurisdictions. In practice, entities with weak AML/CFT controls have already entered and are operating in the EU market by selecting jurisdictions with lighter supervisory practices or previously lower market entry requirements. This regulatory arbitrage has been particularly evident in the lead-up to MiCA, enabling firms to benefit from uneven national approaches until the framework becomes fully applicable on 1 July 2026. During the transitional period, the risks remain acute. Some of those CASPs could also allow unauthorised entities to provide crypto-asset services through hidden partnerships or by selling their business to new unlicensed owners (in effect 'selling' their registration or licensing). This prolongs the EU financial system's exposure to ML/TF vulnerabilities.

1.3 Exploitation of the reverse solicitation exemption

CAs have identified instances where firms improperly relied on or dishonestly used reverse solicitation to offer crypto-asset services within the EU. In some cases, these providers engaged in marketing or pre-contractual discussions that blurred the lines between genuine reverse solicitation, which is possible only in exceptional circumstances according to the guidelines on reverse solicitation([14]) and active solicitation, circumventing regulatory oversight.

Use Case 4. A third country entity appeared to have sought to avoid regulatory oversight by structuring their offerings in a manner to give the impression that business relationships with EU-based clients were initiated solely at clients' own initiative. Its website included several features that indicated a targeted approach towards residents of specific EU MSs.

[13] See clarification provided in ESMA_QA_2086.

[14] See ESMA35-1872330276-2030.

Third country CASPs exploiting the reverse solicitation exemption may create significant ML/TF risks, even under the new regulatory framework. By relying on this exemption, entities with inadequate AML/CFT controls may gain access to the EU market without undergoing proper authorisation and supervisory scrutiny. If not rigorously monitored and enforced, reverse solicitation risks becoming a loophole within the MiCA and AML/CFT framework.

1.4 Weaknesses in AML/CFT compliance and risk management

AML/CFT obliged entities are required to establish and maintain policies and procedures to ensure the effective detection and prevention of ML/TF. These policies and procedures must be proportionate to the nature and level of risk to which each entity is exposed. Inspections carried out by many CAs revealed serious and recurring shortcomings in several areas of the firms' AML/CFT policies and procedures. In addition, CAs found that the AML/CFT procedures described in CASP or issuer application files were not always effectively implemented in practice.

For example, a recurring trend concerns over-reliance on group-wide outsourcing arrangements that fail to account for EU-specific AML/CFT obligations.

Use Case 5. During a supervisory engagement with an EU-based establishment of a third country CASP, a CA identified significant deficiencies in the entity's outsourcing and delegation arrangements. Key AML/CFT functions – including customer due diligence, transaction monitoring and suspicious activity reporting – were performed by the CASP's head office or other group entities located outside the EU, under group-wide policies that were not tailored to EU regulatory requirements. The outsourcing arrangements lacked sufficient contractual clarity, particularly in defining responsibilities, accountability, and compliance with EU AML/CFT obligations. There was no evidence of effective oversight by the EU establishment, and local management had limited understanding or control over the outsourced processes.

Supervisors also observe persistent weaknesses in core AML/CFT controls and risk assessments, with firms also failing to update frameworks to reflect new risks.

Use Case 6. An entity licensed in several EU MSs had failed to verify customer identities properly, did not apply enhanced due diligence for high-risk clients, and lacked effective sanctions-screening tools. Its outsourcing arrangements were generic and did not cover AML/CFT responsibilities, while required reports, including suspicious activity reports, were either missing or of poor quality. Additionally, the CASP had no formal staff training on ML/TF risks and had not updated its risk assessment to reflect new products or geopolitical developments.

Another example relates to insufficient resourcing and instability of the AML/CFT compliance officer role, which undermines effective oversight.

Use Case 7. In the course of assessing a CASP's application for authorisation under MiCA, the supervisory authority encountered concerns related to the stability and adequacy of the firm's

arrangements for the AML/CFT compliance officer role. Since its prior licensing under the national regime, the entity had experienced multiple changes in the AML/CFT compliance officer function, including interim and deputy appointments, which the entity attributed to the competitive nature of the market. As part of its MiCA application, the entity proposed appointing a part-time AML/CFT compliance officer sourced through a consultancy with multiple existing obligations across other institutions and a limited weekly commitment, to serve on an interim basis. This proposal raises concerns about the individual's availability and technical commitment to fulfilling the obligations associated with the said function, particularly in light of the critical nature of the AML/CFT compliance officer role.

Firms are increasingly challenged by emerging technologies and DeFi-related risks, where exposures are underestimated or ignored.

Use Case 8. In one case, an entity with significant exposure to higher-risk products and services, namely unregulated services like DeFi, failed to recognise its role as an entry (on-ramp) and exit (off-ramp) point to and from the decentralised crypto ecosystem. In particular, it had not adequately reflected the associated risks in its internal policies and procedures, including in its individual customer risk assessment and overall business risk assessment methodology. These weaknesses later materialised and the CASP was exploited to channel illicit flows into and from DeFi protocols.

Use Case 9. An EU entity applied to issue EMTs, with funds received in exchange for these tokens to be invested and business clients responsible for distributing them to end customers. As the entity will not have visibility over ultimate beneficiaries, and given the risks associated with redemptions to self-hosted wallets, the CA required specific controls to mitigate these risks. These include enhanced due diligence on all business clients, verification of wallet owners before processing redemptions, and the use of blockchain forensics to trace high-risk or sanctioned addresses. In addition, client-specific transaction limits must be applied, with stricter thresholds for higher-risk clients or jurisdictions, alongside ongoing monitoring to ensure compliance with EU and international sanctions lists as well as internal whitelists and blacklists.

Finally, supervisors note serious deficiencies in reporting, record-keeping obligations, and a lack of implementation of the Travel Rule obligation, particularly among smaller or niche actors such as Crypto-ATM operators.

Use Case 10. A Crypto-ATM operator failed to report above-threshold transactions correctly, submitting incomplete data on incorrect forms. Quarterly statistical reports were inaccurate, with missing or false information on AML/CFT risk assessments, AML/CFT Compliance Officer appointments, transaction monitoring, customer analysis and reporting activity. Additionally, the Crypto-ATM did not implement Travel Rule requirements.

Where CASPs or issuers display weaknesses in their AML/CFT compliance and risk management frameworks, the likelihood of being exploited for ML/TF purposes rises significantly. For example, one major vulnerability lies in exposure to sanctioned individuals or jurisdictions([15]). Ineffective sanctions-screening tools and weak internal processes for resolving alerts reduce the chances of identifying true matches against sanctions lists. In the absence of robust systems and with deficient internal controls, CASPs may unknowingly process prohibited transactions, violating international sanctions regimes and facilitating the flow of illicit finance. Equally, failure by crypto companies to implement the Travel Rule requirement significantly increases the ML/TF and sanctions risk. Without mechanisms to transmit required originator and beneficiary information for cross-border transactions, CASPs create blind spots that allow illicit actors to move funds anonymously and evade detection.

Weaknesses also arise from inadequate intra-group outsourcing arrangements, which create compliance blind spots and accountability gaps. Many newly established entities, particularly smaller ones with limited staff or expertise, rely heavily on group-level operational structures to meet their compliance obligations. However, when EU-based branches of third country CASPs outsource critical AML/CFT functions to parent or group entities outside the EU without clear responsibilities, accountability, or effective EU oversight, compliance with EU rules may not be ensured. This undermines the detection of suspicious activities and weakens supervisory effectiveness.

The instability and limited capacity of the AML/CFT compliance officer function in several CASPs further compound these risks. High turnover, coupled with the appointment of AML/CFT compliance officers who dedicate minimal time or divide their responsibilities across several institutions, results in insufficient oversight and weak governance of AML/CFT frameworks. In some cases, CAs found that AML/CFT compliance officers had insufficient knowledge about crypto-asset-specific risks and blockchain analytical tools management. Among other things, this diminishes the quality of monitoring and creates blind spots in the escalation of suspicious cases. If widespread, such practices reduce the resilience of the sector and heighten the risk of illicit funds moving undetected through CASPs, threatening the integrity of the EU's financial system.

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.

1.5 Unclear beneficial ownership and governance structures

CAs observed vulnerabilities in VASPs/CAPSs and issuers' beneficial ownership structures that seem to be pervasive across the sector. According to CAs, opaque governance and overly complex group structures meant that AML/CFT CAs struggled to identify which entity of a global group was responsible for service provision within their MS, and who the ultimate beneficial owner was. In

[15] See EBA/Op/2025/10.

[16] See EBA/GL/2024/01 for further clarity on the risks and expected controls for obliged entities' interactions with DeFi.

several cases, CAs noted discrepancies between information submitted by the same entity to supervisors in different EU jurisdictions, and between information provided to them by the entity and that entity's official documentation.

Use Case 11. A VASP applying for a licence under MiCA in several MSs provided inconsistent information to different CAs across the EU. This information was also inconsistent with public records. For example, the applicant indicated to one CA that it was incorporated under the laws of a third country but this was not confirmed by that third country's CA. The same applicant VASP was found by another CA to be jointly run by more than 20 distinct entities that were largely established outside the EU and outside regulatory oversight.

Where CASPs or issuers operate with overly complex or opaque ownership and governance structures, several ML/TF risks emerge, including under the new regulatory framework. One major concern is the obscuring of ownership and accountability. Arrangements such as multilayered ownership chains, nominee shareholders, or the use of legal arrangements such as trusts can make it difficult for authorities to identify the individuals who ultimately control or direct an entity. This opacity may be deliberate, to avoid regulatory scrutiny and conceal the origin, control or purpose of the business.

Such complexity also facilitates cross-border ML/TF risks. Inconsistent or incomplete ownership information across jurisdictions creates gaps in supervision, while fragmented oversight of group entities allows risks to accumulate unchecked. Entities operating across borders can exploit these weaknesses to avoid effective regulatory oversight and increase exposure to illicit financial flows.

In addition, opaque structures enable the misuse of front or shell companies. Entities without genuine economic activity can act as vehicles to channel illicit funds under the guise of legitimate transactions. For example, unexplained capital may be injected into the entity through intra-group transfers, masking the true source of funds and complicating detection by financial institutions and supervisors.

Finally, risks are heightened when offshoring or outsourcing is conducted without sufficient transparency. CASPs may delegate AML/CFT-critical functions – such as customer onboarding or transaction monitoring – to affiliates or third parties in jurisdictions with weaker or non-existent regulatory standards. This limits the ability of CAs to verify that safeguards are applied consistently across operations, further reducing the effectiveness of supervision.

1.6 Multi-entity arrangements with high-risk entities

CAs identified cases where entities used linked entities – either through ownership, partnerships, or service agreements – to maintain market presence while avoiding direct regulatory scrutiny. This took different forms:

- *VASPs providing services through another VASP entity in the same MS.* In some cases, VASPs that were unsuccessful in obtaining a registration or licence in a MS acquired substantial shares in another VASP that was already registered or licensed in that MS.

Use Case 12. Following its failure to secure regulatory approval and after receiving an order to cease operations for offering services to national customers without registration, a VASP ceased its operations in the country but transferred local clients to another entity licensed as a VASP in that same MS. At the same time, it acquired shares in that other VASP but remained just below the qualifying holdings threshold. The CA then focused supervisory efforts on the partner VASPs.

Use Case 13. A CA was informed that a non-registered VASP had bought all shares of a locally registered VASP. The CA then discovered indicators that the actual Ultimate Beneficial Owner (UBO) of that VASP was not disclosed in the registration procedure of the local VASP at the time, and that control had been exercised by persons other than those indicated, namely by close associates in the non-registered VASP. Previously, the non-registered VASP had attempted to obtain registration in that MS but had withdrawn from the process after being informed that the CA would refuse the application.

- *VASPs providing services through other VASPs in a different MS.* VASPs failing to obtain registration/licence in a MS continued to serve the citizens of that country through other entities established in a different MS, albeit not benefiting from passporting provisions. This was possible through specific national regimes with a flexible approach to service provision from another EU MS.

Use Case 14. Following an order to cease operations of a non-registered VASP that was offering services to national customers through entities that are not established in EEA countries, the entity moved its local customers to its subsidiary licensed in another MS and continued to provide services in that country, as allowed by its national regulation.

In addition, firms might establish or obtain shares in payment institutions, e-money institutions, and credit institutions, or purchase shares in them, to secure certain core operations in a MS. In certain cases, this can be to provide specific solutions (e.g. e-money wallets, payments), to perform services (e.g. compliance tasks), or even to expand the business scope to other financial services.

Use Case 15. In a MS, an EMI has been identified as providing an e-money wallet solution to a VASP's customers to enable the purchase and redemption of crypto-assets. The e-money wallet solution included a relationship with another institution acting as the VASP's fiat-to-crypto payments company, whereby it conducted certain AML/CFT activities, on an outsourced basis, on behalf of the EMI. This relationship was ultimately ended following the CA engagement and the entity's identification of significant deficiencies in its AML/CFT framework due to the controls outsourced.

Use Case 16. A non-registered crypto-assets business attempted to conduct operations in a jurisdiction through founding companies and by attempting to acquire a majority stake in a bank, which was rejected by the CA due to suitability concerns.

Use Case 17. A CA was contacted by a non-registered crypto-assets business with a view to possibly establishing an EMI. After having reviewed preliminary documents, the CA informed the business that the proposed shareholding structure was not acceptable.

Where CASPs or issuers and their affiliated entities operate through multi-entity structures without adequate transparency or group-level oversight, several ML/TF risks arise, which also affect the effectiveness of the new regulatory frameworks. One key vulnerability is the potential for entities to circumvent supervisory action. Linked or affiliated firms may be used to maintain a market presence even after enforcement measures are taken, enabling the continued provision of services while avoiding scrutiny and ultimately weakening the impact of supervisory interventions. Moreover, the monitoring of such entities poses additional challenges because blockchain records do not distinguish between affiliated entities, which means that NCAs may face difficulties in identifying which specific entity a given activity originates from.

Such structures also perpetuate high-risk cultural practices across affiliated entities. Entities with elevated ML/TF risks may establish or partner with other financial institutions – such as EMIs or PIs – that themselves display weak governance, inadequate AML/CFT procedures, or problematic ownership arrangements. This can entrench poor compliance practices across a wider group and allow risks to spill over into the broader financial system.

Operational vulnerabilities also increase when AML/CFT-relevant functions are outsourced to third parties or group entities operating in less regulated environments. Without strong oversight, safeguards may be inconsistently applied or entirely absent, creating blind spots that allow ML/TF risks to go undetected.

Finally, multi-entity structures heighten risks linked to stablecoins. Even where those stablecoins are issued in compliance with MiCA, trading them on platforms operated by CASPs with inadequate AML/CFT frameworks can compromise the integrity of transactions. Weak secondary market monitoring or insufficient controls may enable illicit funds to circulate through ostensibly compliant instruments, undermining the safeguards established at the issuance stage and eroding trust in wider market integrity.

Use Case 18. A EMT issuer entered into a partnership to facilitate transactions through the platform of a VASP that had been identified by several MSs as having serious deficiencies in its AML/CFT framework. Such an arrangement subjected the EMT to risks stemming from inadequate controls at the counterparty.

Use Case 19. A legal entity issued, on behalf of a CASP already subject to serious penalties for AML/CFT breaches, a stablecoin in a third country. The firm was penalised by the local supervisor and forced to cease issuing the said token due to significant shortcomings in its AML/CFT framework. The CA found the firm had relied on unverified assurances by the partner CASP, had failed to detect illicit activity, and showed broader weaknesses in customer due diligence and investigations.

Earlier this year, a group entity completed the acquisition of a licensed EU EMI, thus extending the operations in the EU, whereby the EU subsidiary issues an EMT that is marketed as fungible with the stablecoin issued by another group entity in another third country. The EU entity has been identified as lacking effective AML/CFT procedures, including deficiencies in client due diligence and verification processes, staff training and suspicious activity reporting mechanisms. It also proposes a 'one-leg-out' issuance model, whereby ARTs are issued under the EU licence while a non-EU subsidiary issues identical tokens outside the EEA. This model increases AML/CFT risks, as non-EU-issued tokens are indistinguishable from EU-issued ones, potentially enabling regulatory arbitrage and the circumvention of MiCA and AML/CFT safeguards. In addition, the cross-border issuance and potential redemption of self-hosted wallets heighten the risk of misuse for illicit activity, underscoring the need for robust controls to mitigate AML/CFT exposure. Its license was also revoked.

2. The new framework introduces safeguards, but competent authorities should pay attention to specific ML/TF factors to ensure its effective implementation

MiCA, together with amendments to the AMLD and the upcoming implementation of the new AML/CFT regulatory frameworks, establishes a more robust and harmonised EU-wide regime for the authorisation, supervision and governance of crypto-assets businesses. This comprehensive framework aims to close existing regulatory gaps, prevent arbitrage across MSs, and strengthen AML/CFT safeguards throughout the sector. Despite the safeguards introduced, effective implementation by CAs will be critical in ensuring that the new regulations are applied and enforced across MSs consistently. As set out in Section 1 of this report, many of the ML/TF risks remain relevant and may affect the effective implementation of the enhanced MiCA and the new AML/CFT frameworks, particularly in relation to authorisation, operational transparency, AML/CFT compliance, supervisory cooperation, and control of complex ownership structures.

2.1 An EU-wide authorisation and passporting regime with enhanced supervisory powers

MiCA establishes a comprehensive EU-wide authorisation regime for issuance, trading and service provision of crypto-assets businesses, requiring entities to obtain authorisation from a CA in a single MS to operate throughout the Union. This single authorisation replaces the previous patchwork of national licences or registrations and is granted based on harmonised prudential, organisational, governance and AML/CFT standards designed to prevent regulatory arbitrage and enhance legal clarity and predictability. Once authorised, CASPs benefit from passporting rights, allowing them to provide services across MSs either by establishment or cross-border service provision. During the transition period until 1 July 2026, 'grandfathering' provisions allow CASPs authorised under former national regimes to continue operations only within their original MS, without passporting rights, thus limiting backdoor cross-border activities. This harmonised approach reduces the risk of firms exploiting lenient national frameworks. Nevertheless, it also implies that risks or non-compliance in one MS can propagate across borders via the passporting mechanism.

In addition, there are now strict limits on reverse solicitation. MiCA only allows third country CASPs to provide services if initiated exclusively by the client([17]). Any marketing or solicitation in the EU voids this exemption. The Regulation explicitly bans indirect promotion (e.g. through affiliates or intermediaries) intended to exploit the reverse solicitation exemption. This closes off common strategies that previously allowed firms to circumvent the spirit of EU rules while formally remaining

[17] See ESMA35-1872330276-2030.

outside the regulatory perimeter. Equally, CAs are empowered to detect and act against unauthorised services provided under false claims of reverse solicitation, thereby preserving regulatory integrity.

An essential safeguard of the new framework lies in the strong enforcement powers available to CAs, the EBA, ESMA and AMLA to ensure compliance with anti-financial crime obligations. Under MiCA, infringements can trigger administrative measures (including withdrawal of the authorisation) and it requires MSs to provide effective, proportionate and dissuasive sanctions for non-compliance. Supervisors, including the AMLA, will be able to impose corrective measures and fines where CASPs within their remit fail to meet harmonised requirements. For issuers of significant ARTs and EMTs, the EBA is required to consider whether an infringement has occasioned, facilitated, or is otherwise attributable to ML/TF risks when taking supervisory measures.

Lessons learned from the previous regime and existing cases under the new regime suggest that the following considerations will be key to ensuring that the new EU framework is applied effectively, preventing past risks from re-emerging.

Definition of exit strategies for unauthorised CASPs post-grandfathering

As the transitional period for VASPs comes to an end, national authorities may need to consider how to ensure a controlled exit of entities that are currently operating in their Member State but have not obtained MiCA authorisation. As set out above, CAs need to be mindful of unsuccessful businesses potentially exploring ways to regain market access, such as reverse solicitation, spillover to self-hosted wallets, or transferring activity to entities in other MSs with extended transitional periods.

Examples of measures CAs have taken include the preparation of contingency plans for client migration, safeguarding customer assets, as well as compliance with AML/CFT obligations. Examples highlighted in this report also suggest that coordination between home and host supervisors, including the EBA, ESMA and AMLA where relevant, will remain important to enable supervisors to monitor the market, close regulatory gaps, and prevent unauthorised CASPs from continuing to provide cross-border activities.

Monitoring the perimeter for unauthorised activities

CASPs and issuers operate in a highly dynamic and often decentralised way. This means that it is essential for CAs to monitor activities in the market to ensure that all entities that provide regulated services in their jurisdiction are duly authorised. CAs currently use advanced data analytics and intelligence-sharing with other jurisdictions to enhance their ability to detect unauthorised or suspicious crypto activities. Regular audits, market surveillance and public reporting mechanisms also play an important role in this process. Other examples of the tools CAs use include:

- national account registers to detect changes in financial activity or affiliates involving local institutions;
- regulatory return analysis to search for material growth;
- surveys on market exposure to specific CASPs raising ML/TF concerns;

- customers' complaint mechanisms referring to alleged violations of transparency/disclosure obligations and alleged fraud and ML;
- inspections of linked entities to assess ML/TF risks and the independence of those entities in relation to the targeted CASP or issuer;
- use of blockchain analytical tools in order to check the volume and nature of the crypto-assets services provided and assess the ML/TF risks of their activities.

Consumer protection measures can also support perimeter monitoring. Some CAs conduct consumer outreach campaigns and publish warnings about unauthorised actors. They also share alerts issued by other CAs, the ESAs and, in the future, AMLA, to inform the public about risks associated with crypto activities and unauthorised entities. These efforts help prevent consumer harm and reinforce market integrity.

Ensuring the adequate application of the MiCA authorisation procedure on entities with legacy AML/CFT issues

Where entities were already licensed or registered in a MS, CAs generally have access to the supervisory history of those entities. In certain cases, entities identified at national level as highML/TF risk have obtained MiCA authorisation despite unresolved AML/CFT issues.

Use Case 20. In one MS, a VASP operating under national law applied for MiCA authorisation in the same jurisdiction. The entity was classified by supervisors as high-risk and had several ML/FT vulnerabilities, including pending enforcement actions for inadequate AML/CFT systems and controls. Despite these unresolved issues and the availability of a long grandfathering period under national rules, the entity was authorised shortly after MiCA's entry into application.

Use Case 21. A CA intervened against an issuer of ARTs already operating in the country before 2025 after identifying serious shortcomings during the MiCA authorisation process. These included weak governance and risk controls, opaque ownership structures with links to high-risk third countries' entities, and breaches of AML/CFT obligations. The authority imposed immediate measures and the company is now considered liquidated.

Authorising firms without adequately addressing legacy ML/FT concerns increases future oversight burdens, and weakens the EU's anti-financial crime defences. This is relevant in particular because for the first time, includes passporting provisions which means that, once authorised, CASPs can legitimately provide their services in different MSs. As a result, unresolved ML/TF risks are not contained within a single jurisdiction and may spread to other MSs.

Authorities should, therefore, ensure that thorough ML/TF risk assessments are conducted before granting authorisation. This may include reaching out to CAs in other MSs that may have insights into the entity's prior operation. Where serious ML/FT issues are identified or remediation is outstanding, authorisation should not be granted until they are adequately mitigated or resolved in line with EU standards and expectation.

2.2 Integration into AML/CFT framework and enhanced AML/CFT obligations

Entities operating under MiCA are subject to AML/CFT obligations and must implement measures to prevent their platforms and services from being used for financial crime purposes. This includes assessing and understanding the ML/TF risk to which they are exposed, and putting in place internal policies, controls and procedures that are adequate and commensurate to that risk. Issuers of ARTs that are not CASPs or other obliged entities specifically are not subject to specific AML/CFT systems and controls rules but still have to ensure that the issuer or the sector are not exposed to serious ML/TF risks and that financial crime is not committed or facilitated.

The EBA Guidelines, including its updated ML/TF Risk Factors Guidelines([18]) provide sector-specific guidance on the steps entities should take to comply. The EBA's([19]) and ESMA's([20]) regulatory technical standards (RTS) specify the documentation and evidence CASPs and issuers must submit during authorisation, including proof of robust internal controls, AML/CFT policies, procedures and risk assessment frameworks. This should ensure that only entities with adequate systems for managing ML/TF risks gain entry to the market, effectively raising the bar for compliance.

Drawing on the lessons learned, the aspects outlined below are key to supporting the effective implementation of those instruments and preventing past risks from re-emerging.

Keeping abreast of developments in controls and ML/TF risks

To ensure the effective application of the new EU AML/CFT framework in the crypto-asset sector, CAs must adopt a dynamic and forward-looking approach to risk management. The pace of innovation, the increasing availability of decentralised technologies, and increasing cross-border complexities require supervisors to be both agile and well-informed. This is particularly relevant in the context of rapidly developing areas – such as DeFi links, products and services, crypto ATMs, and crypto payment cards, etc. – where ML/TF vulnerabilities are evolving and more work is needed to identify and develop effective control mechanisms. This includes, for instance:

- *Ongoing risk identification and assessment.* Supervisors should establish formal processes to regularly review and update their understanding of ML/TF risks in the crypto-asset sector. This includes analysing new typologies (such as, Travel Rule protocols, transaction monitoring, remote onboarding, etc.), changes in service offerings (e.g. new products like crypto-credit cards), and vulnerabilities linked to geopolitical and macroeconomic developments.
- *Structured public–private dialogue.* Regular, transparent communication channels with CASPs and issuers, financial institutions, blockchain analytics providers and information exchange protocols, and dialogue among CAs and the relevant EU authorities help supervisors to understand emerging

[18] See EBA/GL/2024/01.

[19] See, for example, EBA/RTS/2024/03 EBA/ITS/2024/03 for issuers of ARTs.

[20] See ESMA18-72330276-1634.

risks and adjust regulatory priorities. Supervisory roundtables, innovation hubs and thematic workshops can facilitate such dialogue.

- *Joint development of risk indicators and red flags.* Some authorities have co-created typologies and risk indicators with the private sector, improving the detection of high-risk transactions and actors. These outputs can feed into national risk assessments and supervisory focus areas.
- *Training and upskilling of supervisory staff.* CAs should invest in continuous training programmes that include blockchain forensics, DeFi risk mapping, and emerging typologies.
- *Use of SupTech and data aggregation tools.* A number of authorities are experimenting with or deploying SupTech solutions for risk monitoring, such as dashboards that visualise transaction flows, network connections and anomalies. These tools enhance supervisors' ability to stay ahead of fast-evolving ML/TF schemes in the crypto space.

2.3 Heightened transparency, governance and beneficial ownership requirements

A core element of the new AML/CFT framework focuses on enhancing transparency and governance. MSs are required under AMLD6 to maintain accurate, centralised registers of beneficial ownership, facilitating group-wide supervision and enabling supervisors to uncover concealed ownership links. MiCA, AMLR, and AMLD6 collectively mandate rigorous suitability and fitness checks for directors, senior management and qualifying shareholders, ensuring that individuals with a history of ML/TF offences, sanctions or other disqualifying factors are excluded. These checks are reinforced by the Joint EBA-ESMA Guidelines on suitability([21]), which emphasise the importance of cross-border cooperation to prevent inconsistent application of rules from being exploited. Corporate governance under MiCA demands clearly defined and transparent organisational structures with explicit AML/CFT roles and responsibilities to prevent obscured accountability. The EBA's([22]) and ESMA's([23]) RTS, specifying the documentation and evidence that CASPs and issuers must submit during authorisation, further requires disclosure of ownership and governance details during authorisation, allowing supervisors to identify risks from linked or opaque structures upfront. The AMLR broadens the definition of control to include indirect influence and nominee arrangements, requiring supervisors to assess ML/TF risks arising from complex corporate structures. MiCA explicitly targets informal or indirect control by empowering NCAs to intervene even when formal ownership thresholds are not met, closing loopholes that entities might exploit by dispersing influence through related entities or informal arrangements. Supervisors are thus expected to adopt a holistic approach, looking beyond surface-level ownership to fully assess operational and control structures – particularly in multi-entity, offshore or otherwise opaque setups – to identify and mitigate ML/TF risks effectively.

The EU's experience suggests that the following considerations will be key to ensuring that the new EU framework is applied effectively, preventing past risks from re-emerging.

[21] See ESMA35-36-2319 EBA/GL/2021/06.

[22] See, for example, EBA/RTS/2024/03 EBA/ITS/2024/03 for issuers of ARTs.

[23] See ESMA18-72330276-1634.

Overseeing changes in ownership structure and entity (in)dependency

Changes in ownership are underway in several entities to address feedback from supervisors from pre-MiCA shortcomings. Previous findings suggest that CAs should in those cases conduct thorough checks to ensure that the institution's governance and decision-making processes do not encounter hidden or undue influences, particularly when professional or family connections to their predecessors exist.

Use Case 22. In a third country, an entity that also operates in the EU was allegedly linked to a custodian bank, where a close family member of the former CEO held both shareholdings in the bank and other non-qualifying interests. The entity had maintained deposits at the bank, which were withdrawn before the bank was placed under bankruptcy proceedings.

A simple change of senior manager is not a sufficient sign that good governance has been adopted. Therefore, supervisors should make sure that any new office holders – especially in compliance, risk or control functions – are truly independent and autonomous so that these people can act without pressure or interference. This is especially critical for entities with a history of poor compliance culture.

Ensuring adequate and timely reassessment of fitness and propriety

CAs' approaches to assessing the fitness and propriety of directors and senior management or of the UBOs, and to reassessing their fitness and propriety where adverse information emerges, previously diverged. For example, under the regime in place before MiCA, the assessment of the fitness and propriety of UBOs was not always mandated. The rules governing assessment or reassessment of the suitability of an entity's senior management, UBO or majority shareholder were inconsistent in those MSs that required them. For example, in the absence of a criminal conviction, most CAs considered that a reassessment of an entity's senior management or significant shareholders was unnecessary. Where it was considered, it was often limited to the entity's local operations and did not take into account the firm's global structure or the ongoing influence exerted by majority shareholders (or their close associates) on the group and its entities. This divergence led to inconsistent levels of scrutiny and supervision across the EU.

Use Case 23. In one VASP, a series of supervisory actions by third country supervisory authorities for serious AML/CFT systems and controls failures and sanctions evasion triggered the reassessment of an entity's UBO in two MSs. However, in other MSs, where this entity was also registered or licensed, supervisors concluded that the conditions for reassessment in national law had not been met or that the assessment of the fitness and propriety of UBOs was not always mandated.

Experience of supervising VASPs/CASPs to date suggests that cases should also be considered for reassessment where an entity, members of the management body, shareholders and members (whether direct or indirect) that have qualifying holdings stand accused of ML/TF or facilitating ML/TF

through failure to put in place appropriate AML/CFT systems and controls. Therefore, specifically with respect to fitness and propriety assessment where criminal proceedings are ongoing, the ESMA Supervisory Briefing on Authorisation of CASPs under MiCA([24]) states that CAs should take into account ongoing criminal proceedings, even if a conviction or penalty is not yet imposed, both inside and outside the EU. This includes cases of guilty pleas, among others([25]). In order to meet EU supervisory expectations, CAs should adopt a proactive approach by engaging directly with counterparts in the relevant countries to obtain timely and reliable updates, particularly in the context of an ongoing or pending authorisation process. In addition, CAs should carry out a thorough risk assessment of the potential impact on the products and services offered, especially when the operational model involves links to other entities, and where entities that are subject to judicial proceedings form part of that model.

Use Case 24. An entity operating in the EU was investigated by a foreign authority while its EU approval was under review. The entity later pleaded guilty to AML/CFT breaches. Although the CA contacted its foreign counterparts, the potential risks and operational implications of the investigation were not fully considered in the supervisory assessment.

Monitoring linked entities in AML/CFT supervision

CAs should ensure that they identify linked entities to mitigate the risk of these entities serving as conduits for circumventing regulatory requirements. Analysis of linked entities in crypto-assets supervision involves examining the relationships and connections between various entities operating within but also outside the crypto-asset ecosystem. This includes understanding how different players, such as exchanges, wallet providers and other service providers and financial institutions, are interrelated. CASPS can operate through complex networks of linked entities that might obscure true ownership and control structures, making it challenging to assess potential risks.

Use Case 25. Many CAs, when asked by the EBA to assess entities linked to specific CASPs, identified additional relationships that were not apparent through the registered ownership structure alone. These connections were uncovered using other attributes that can associate entities, such as different legal names with specific shared attributes, shared beneficial owners, the same members of the management body or key function holders, among others. This enabled authorities, for example, to assess the independence of close associates and, in some cases, to trigger supervisory actions against linked entities.

Effective supervision therefore requires a thorough analysis of these connections to ensure that all entities involved adhere to regulatory standards and that any risks posed by interconnected operations are adequately addressed. By scrutinising linked entities, regulators can better detect and

[24] See ESMA75-453128700-1263.

[25] See EBA/GL/2021/15.

prevent illicit activities, improve transparency, and enhance the overall integrity of the crypto-asset market.

Use Case 26. A third country EMT issuer, currently implementing a remediation plan to address supervisory actions, partnered with an EU-authorised issuer to issue a fungible token within the EU. Due to the fungibility of the token, some intra-group arrangements may be put in place which may require heightened attention and monitoring of the EU entity's ability to comply with AML/CFT obligations.

2.4 Supervisory cooperation and public transparency

Supervisory cooperation is key to reducing regulatory arbitrage and ensuring a unified supervisory approach. It also makes effective risk-based supervision possible. MiCA and AMLD6 mandate strong information-sharing protocols between home and host supervisors, facilitating consistent authorisation standards and ongoing AML/CFT monitoring across jurisdictions. Additionally, the ESMA maintains a public register of authorised CASPs, enhancing transparency by enabling authorities and the public to distinguish authorised firms from unauthorised or fraudulent operators, thereby deterring forum shopping and misrepresentation.

The following considerations help ensure the new EU framework is applied effectively, preventing past risks from re-emerging.

Focusing on effective cooperation and information-sharing among authorities

According to AMLD6, which applies from 2027, where an obliged entity operates establishments in another MS, the supervisor of the home MS will be responsible for supervising the obliged entity's application of group-wide AML/CFT policies and procedures. Close cooperation among supervisors should be ensured in those cases and is factored into the legislative framework through, for example, the AML/CFT colleges framework and the possibility that some cross-border entities may be directly supervised by AMLA.

Use Case 27. Several non-EU CAs highlighted serious governance and ML/TF issues related to an entity. While some EU CAs had already acted upon the serious developments, others did not follow up with specific steps in their respective jurisdictions, claiming hindrances in their national frameworks. However, where actions were taken, all the CAs identified similar issues which would probably be extended to the remaining EU establishments and branches, should further actions have been taken. Therefore, the entity continued to operate in those remaining countries without any required remediation plan.

Collaboration among authorities is essential to ensuring that ML/TF risks are identified and managed effectively. This applies domestically in relation to AML/CFT authorities, MiCA authorities, prudential supervisors and Financial Intelligence Units (FIUs). Considering the cross-border nature of the sector's

activities, cooperation with the EU and third country counterparties is not only beneficial but also necessary in the supervision of CASPs and issuers.

Cooperation enables the timely exchange of intelligence, the identification of emerging risks and consistent supervisory responses. It is particularly relevant to closing regulatory gaps and preventing regulatory arbitrage where entities might exploit less stringent regulations in one MS to operate at EU level. It is also important because each one of these key authorities has different scopes of information available to them. For instance, supervisors are often well placed to detect governance or compliance failures, while FIUs possess financial intelligence that can reveal suspicious patterns or criminal activity. Strengthening this cooperation is essential to ensuring a holistic view of ML/TF risks and enabling timely intervention.

The EBA's findings show that cooperation between CAs can still be hampered by a series of factors. Obstacles include the number and diverse nature of CAs, which can make cooperation complex or operationally challenging where the nature of the CAs diverges. This is the case, for example, in situations where multiple AML/CFT CAs within the same MS are responsible for the supervision of CASPs and/or issuers, with responsibilities spread across market, conduct, prudential and AML/CFT authorities. In some cases, gateways for information exchange intra and across jurisdictions appear to be missing.

There were successful cases of close cooperation between EU and non-EU counterparties. These were related mainly to AML/CFT authorities that had already registered or licensed a VASP or authorised a CASP, with whom an application was pending, or with authorities that already imposed restrictive measures. Regarding cooperation with non-EU countries, the main counterparties referred to some extended collaboration with the UK as well as US authorities. Equally, some CAs also ensured coordination with prudential counterparties for a holistic approach, mainly regarding the ownership structure – both at market entry and during the monitoring stages – and the entity's strategy for the future. Some others also focused on coordination with the FIUs through regular information-sharing meetings regarding the ML/TF risks associated with the targeted entities and linked entities.

Use Case 28. AMLA and ESAs place a strong emphasis on cooperation. For instance, AMLA has signed a Memorandum of Understanding([26]) with the ESAs, where the authorities have committed to informing each other – particularly in the case of the EBA and ESMA, financial entities under MiCA – of situations where joint action may be required to address specific issues in a comprehensive and effective manner. In addition, AMLAR includes a similar requirement regarding cooperation with non-AML/CFT authorities, specifically other national authorities responsible for ensuring compliance with MiCA. AMLA is also required to facilitate effective cooperation and information exchange between supervisory authorities and FIUs, recognising the complementary nature of their functions.

Ensuring the effectiveness of the Central Contact Point role

[26] See AMLA signs Memorandum of Understanding with the European Supervisory Authorities for effective cooperation and information exchange.

The appointment of a Central Contact Point (CCP)([27]), as provided for under Article 45(9) of Directive (EU) 2015/849, as amended by Regulation (EU) 2023/1113, constitutes an important tool for enhancing supervisory cooperation and ensuring effective oversight of cross-border entities operating within the EU. The CCP mechanism enables host MSs that apply it to require certain obliged entities – particularly those providing services on a cross-border basis without a physical establishment – to appoint a designated point of contact in their jurisdiction. This is the case even if their establishments are not 'obliged entities' themselves.

Experience from CAs highlights both benefits and challenges in implementing the CCP requirement. While it facilitates close supervisory interaction, some CAs report that some CCPs do not have sufficient resources, authority or expertise to perform their duties effectively. Since application of the CCP regime is not mandatory, requirements across MSs can also diverge and increase the compliance burden for cross-border entities. Ensuring harmonised application across jurisdictions will be key to maximising the effectiveness of this mechanism.

[27] See EBA/CP/2024/23.

3. Conclusion

The crypto landscape continues to evolve. The new legislative framework introduces, for the first time in the EU, a comprehensive regulatory regime for issuance, trading and service provision, which has the potential to significantly reduce financial crime risks associated with the sector and enhance the resilience of the EU's financial system, promoting a safer and more transparent market for crypto-assets.

The effective implementation of this framework requires a concerted and joint effort by all CAs to ensure that vulnerabilities and risks are identified and addressed at an early stage. To effectively manage the challenges and ML/TF risks associated with crypto-asset service provision, CAs should draw on the lessons learned from this report. The regulatory instruments issued by the EBA and ESMA provide essential support in this regard, and ongoing coordination and information-sharing between CAs remain critical to ensuring a harmonised approach across the EU.

Given the sector's dynamic and fast-evolving nature, consistent and robust approaches across CAs are essential to achieving convergence from the outset. As most CAs are currently authorising CASPs and issuers, fostering trust in this high-risk sector is critical. The authorisation process should therefore act as an effective gatekeeper, allowing CAs to verify compliance with regulatory requirements and ensure that key risks inherent in CASP and issuers' business models are effectively managed before granting the authorisation.

The EBA will transfer its standalone AML/CFT powers and tasks to AMLA by the end of 2025. Nevertheless, it will continue to play a key role in the crypto sector through its MiCA mandate, supporting the fight against financial crime, promoting supervisory convergence, and ensuring that emerging risks are promptly addressed.

European Banking Authority

Tour Europlaza, 20 avenue André Prothin CS 30154
92927 Paris La Défense CEDEX, FRANCE
Tel. +33 186527000

E-mail: info@eba.europa.eu

https://eba.europa.eu