MICAR ROUNDTABLE EXPERT SERIES

Madrid

Initiated by Dr. Nina-Luisa Siedler and Mariana de la Roche W., the MiCAR Roundtable Expert Series continues to build legal clarity within the EU's evolving regulatory framework for crypto-assets under MiCAR.

The eighth roundtable in this series was hosted at the historic Palacio de Cibeles in Madrid on October 10th, 2024. We are deeply grateful to our partners and supporters who made this event possible: the European Commission, Crystal Intelligence, Merge Madrid, and Taxbit.

The Madrid session brought together key players from the regulatory and crypto sectors to explore essential topics related to MiCAR. The discussions were led by contributions from Tommaso Astazi, who examined the integration of the Transfer of Funds Regulation (TFR) with MiCAR; Max Bernt, who addressed privacy and data protection challenges across MiCAR and other regulatory frameworks; and Albi Rodriguez Jaramillo, who discussed the compliance requirements and systemic risks associated with E-Money Tokens (EMTs).

This report consolidates the insights gathered during the Madrid discussions. It is essential to note that the perspectives and conclusions presented here represent the collective understanding of these topics and do not reflect the individual positions of any participants or rapporteurs.

1. **Expanding the Regulatory Landscape: TFR and Its Integration with MiCAR**

Tommaso Astazi, Head of Regulatory Affairs at Blockchain For Europe, began the presentation by emphasising that the EU regulatory framework for crypto-assets not only includes MiCAR but also incorporates other critical legislation, notably the Transfer of Funds Regulation (TFR) as part of the AML package. The TFR aligns with FATF Recommendation 16, expanding the "Travel Rule" to the crypto sector, requiring CASPs to exchange information about the originator and beneficiary of each crypto transaction they facilitate. Under this rule, whenever a CASP is involved in a transaction, it must collect and transmit the originator and beneficiary information. This process is straightforward for transfers between two CASPs, as both have established customer relationships (including KYC verification).

However, the landscape becomes more complex when transactions involve self-hosted wallets (SHWs). Transfers between a CASP and an SHW raise complications in the collection and verification of information related to the originator and beneficiary since SHW providers typically do not verify user identities through KYC processes. Negotiations to finalize the TFR in June 2022 led to a compromise, allowing CASPs to forego mandatory identity verification for SHWs under certain thresholds. For transfers under €1000, a simple information collection is required, while transfers above €1000 to a user's own SHW mandate CASP verification of wallet ownership. Above this threshold to a third-party SHW, CASPs can apply a risk-based approach to determine the appropriate due diligence measures.

Nevertheless, the European Banking Authority's (EBA) recently released Travel Rule guidelines appear to deviate from this political agreement by suggesting CASPs may need to gather "additional data from other sources to verify" third-party SHW information. This shift could force many CASPs to halt transfers above €1000 to third-party SHWs, disrupting user access to compliant transactions and potentially pushing activity toward unregulated markets, contradicting the TFR's intent.

Discussion Highlights

1. Regulatory Clarity: Participants emphasised that developing Level 2 measures under MiCAR and TFR should ensure regulatory clarity

without reintroducing the discarded verification requirement. The political compromise acknowledged that a mandatory verification for SHWs could not only be impractical but would create data security risks by fostering databases vulnerable to cyber threats. Stricter rules would deter CASPs from offering transfers to third-party SHWs, moving transactions toward unregulated markets – counterproductive to the legislative goal of increased oversight.

2. KYC-Compliant SHWs and Technological Innovations: New wallet solutions incorporating privacy-enhancing technologies (such as decentralized identities, ZKPs, and decentralized KYC tokens) could offer a balanced solution, allowing CASPs and law enforcement to identify wallet owners when necessary. This approach aligns with the TFR's political language, aiming to support technology capable of verifying SHW ownership on an as-needed basis.
3. Current Industry Solutions: There are existing and emerging technological tools that enable secure information exchange and third-party verification, such as Notabene's solution, which facilitates identity verification requests for third-party wallets via secure messaging. Solutions like these support CASPs in fulfilling verification requirements without compromising user privacy.
4. Misconceptions of Web3 Risk: Applying the Travel Rule – originally designed for the traditional financial (TradFi) sector using SWIFT – directly to Web3 without adaptation overlooks the technological differences between these spaces. Participants argued that regulatory scrutiny over crypto-transfers should not exceed that applied to cash transactions, which remain far less traceable. Blockchain analytics already provide a robust method for tracking illicit activities, offering more transparency than equivalent mechanisms in the TradFi space.
5. Risk-Based Approach and Flexible AML Solutions: The roundtable reaffirmed the importance of a risk-based approach, allowing CASPs to assess individual transactions based on risk, using transaction monitoring and blockchain analytics for a

proportionate response. This approach respects users' privacy while ensuring regulatory goals are met.

unique characteristics of the Web3 ecosystem and the regulatory goals of MiCAR and TFR, ensuring a balanced approach to AML compliance in crypto

This session underscored the need for regulations that accommodate both the

Primary Calls to Action for Expanding the Regulatory Landscape: TFR and Its Integration with MiCAR

The primary calls to action based on the discussions are:

- **Reinforce the Risk-Based Approach:** Regulators should uphold a risk-based framework, enabling CASPs to tailor services based on their risk tolerance and the specifics of each transaction, rather than imposing blanket requirements.
- **Support Technological Solutions:** Regulatory frameworks should allow for and promote technological innovations that enhance compliance while protecting user privacy. Tools like identity-on-demand solutions can help maintain compliance without excessive user data collection.
- **Clarify SHW Verification Thresholds and Standards:** Regulators need to offer clear guidance on thresholds for enhanced due diligence and establish ID standards that work with evolving digital identity solutions, ensuring consistent and practical application across the EU.
- **Avoid Stricter Rules than in TradFi:** Treating crypto-transfers as inherently riskier than cash transactions lacks a factual basis. Regulations for blockchain-based assets should be proportionate to the transparency and traceability that blockchain provides.

2. E-Money Tokens and Systemic Risk: Ensuring Compliance and Financial Resilience under MiCAR

Albi Rodriguez Jaramillo, Law Consultant at Garrigues, presented an in-depth analysis of E-Money Tokens (EMTs) under MiCAR, discussing their systemic importance and the regulatory requirements necessary to mitigate potential risks. He began by highlighting how tokenized money, which operates on Distributed Ledger Technology (DLT), has transformed aspects of the financial system, offering increased efficiency, transparency, and cost reduction across wholesale and retail markets.

Stablecoins have become a significant component in the tokenized money market, acting as a bridge for crypto investors to enter and exit the market efficiently. However, as Rodriguez noted, not all stablecoins are built alike, varying widely in their regulatory and operational standards. He pointed out that with substantial market capitalizations—Tether at $119 billion and USDC at $35.8 billion—these stablecoins play a key role in transactions, with daily volumes rivalling even major cryptocurrencies like BTC and ETH.

Under MiCAR, EMTs are defined as digital representations of value intended to maintain parity with a single official currency, effectively serving as electronic surrogates for traditional money. These tokens must be issued by authorised institutions within the EU, ensuring holders can redeem them at any time at par value with the reference currency. MiCAR also introduces the designation of Significant EMTs, which bear heightened regulatory scrutiny, particularly if they reach certain thresholds in transaction volume, market capitalization, or interconnectedness with the financial system.

Rodriguez referenced the EBA's recent supervisory priorities for ART/EMT issuers, which emphasise financial resilience and effective risk management. He highlighted how MiCAR's own funds and reserve requirements are essential to EMT issuers' financial stability and that EMTs classified as "Significant" require stringent capital and liquidity buffers, regular stress testing, and detailed reporting to both NCAs and the EBA.

Challenges in Reporting and Supervision Coordination

Rodriguez Jaramillo underscored the complexities in EMT reporting, especially

with different supervisory bodies at both the EU and national levels. As EMTs interact heavily with CASPs (Crypto-Asset Service Providers), issues arise from differing standards and real-time supervision requirements. The dual supervision model for Significant EMTs—overseen by both NCAs and the EBA—adds further complexity to aligning processes and ensuring prompt, harmonised reporting.

To address these issues, Rodriguez advocated for stronger technological solutions, such as Supervisory Technology (SupTech) tools like BIS Pyxtrial, to streamline data integration across NCAs, enhancing the efficiency and reliability of EMT supervision. He emphasised the need for uniform data reporting standards and specialised regulatory personnel to handle these emerging technologies and complex reporting requirements.

The discussion around the proposed Solutions by the roundtable included

1. Reliable Reporting Mechanisms: EMT issuers should implement verifiable reporting protocols that integrate data from authorised providers.
2. SupTech Adoption for Real-Time Supervision: Tools like BIS Pyxtrial could standardise reporting, giving regulators a centralised view of EMT health and compliance.
3. Enhanced Capacity Building: Establish standardised training programs across the EU to equip regulatory staff with the necessary technical and legal expertise, with funding supported by EU Digital Transformation grants.
4. Improved CASP Collaboration: CASPs should be proactive in sharing relevant information with regulators, especially for systemic EMTs.

Roundtable Discussion Highlights

Participants acknowledged the inherent complexity of regulatory coordination for systemic EMTs, noting the valuable role SupTech could play in managing cross-jurisdictional reporting. The discussion emphasised the need for regulatory clarity to avoid redundant or excessive reporting, while also allowing for regulatory flexibility during the initial implementation phase. Capacity building within regulatory bodies was widely agreed upon as crucial for effective oversight of EMTs, as was fostering a productive dialogue with CASPs to ensure

the collection of relevant, not excessive, data.

The roundtable concluded that clear, harmonised compliance standards and a focus on leveraging technology, particularly SupTech, are essential to effectively manage systemic risks associated with EMTs. Events such as this roundtable, facilitated by De La Roche W. Consulting and Siedler Legal, play a vital role in fostering a shared understanding of regulatory challenges and solutions across the EU.

Primary Calls to Action on E-Money Tokens and Systemic Risk

The primary calls to action based on the discussions are:

- **Enhance Reporting Consistency through SupTech Tools:** Regulators should actively adopt SupTech solutions like BIS Pyxtrial for real-time, consistent, and centralised supervision of EMTs. This would ensure that reporting is both harmonised and capable of addressing the complexities unique to systemic EMTs.
- **Standardise Regulatory Training Across the EU:** Establish an EU-wide training program to build regulatory capacity on EMT supervision, equipping staff with the necessary expertise in emerging financial technologies. This program should be funded through EU Digital Transformation grants.
- **Clarify Compliance Standards for EMT Reporting:** Regulatory authorities should provide clear guidelines on reporting obligations for EMT issuers, particularly for those classified as Significant EMTs. This includes defining the data requirements and thresholds to prevent redundant reporting and to streamline compliance.
- **Promote CASP Collaboration in Data Sharing:** Encourage Crypto-Asset Service Providers (CASPs) to collaborate closely with regulators, ensuring timely and relevant information sharing for effective supervision. This partnership would also support adherence to MiCAR's risk and liquidity standards.

3. Addressing Privacy and Data Protection Challenges within MiCAR, AML, DAC8, and CARF Frameworks

Max Bernt, Managing Director, Europe at Taxbit, provided an in-depth examination of the privacy and data protection challenges faced by Crypto-Asset Service Providers (CASPs) under the increasingly complex reporting obligations imposed by regulatory frameworks like MiCA, AMLD6/AMLR, TFR, DAC8, and CARF. He identified key concerns arising from these obligations, including data handling risks, inadequate tools for investigation, and cross-border data-sharing complexities, all of which put CASPs at heightened risk of privacy breaches and regulatory non-compliance.

One significant issue is the process of combining on-chain public data with off-chain private data for compliance purposes. This integration introduces notable privacy risks, including potential data leaks, breaches of tax secrecy, and exposure of sensitive personal information. Although tools like Crystal, Chainalysis, and TRM Labs are commonly used to manage data, improper handling can violate user privacy rights.

Another challenge relates to the use of inadequate tools for conducting sensitive investigations. Regulatory bodies have sometimes relied on insecure, non-specialized tools (such as retail-grade web applications) for tax or AML investigations. These tools often lack robust encryption, access control, and advanced security measures, making CASPs vulnerable to unauthorised access and data exposure.

A third concern centres on cross-border data-sharing, particularly under frameworks like DAC8 and CARF, which facilitate extensive exchanges of crypto-related user data across borders. Bernt noted that insufficient guidelines are provided for secure handling of such information, especially when data is repurposed for non-tax uses, such as AML or counter-terrorism efforts, increasing risks to data privacy.

Finally, the expanding scope of reporting obligations under DAC8 and AMLD6 raises concerns about potential violations of individual privacy and data protection rights. Combining on- and off-chain datasets without adequate privacy safeguards may expose sensitive data, creating legal uncertainty and raising the

risk of infringing fundamental privacy rights.

To address these challenges, Bernt recommended several key solutions. Firstly, he advocated for stricter regulatory oversight on reporting tools, suggesting that authorities require the use of government-certified platforms for handling sensitive off-chain data during tax and AML investigations. Closed cloud solutions, he argued, offer higher privacy standards through robust encryption, security auditing, and controlled access.

Secondly, Bernt emphasised the need for a clear separation between on- and off-chain data in regulatory frameworks. He proposed developing protocols to manage these data types independently, incorporating specific safeguards to protect off-chain data when combined with on-chain analytics.

He further recommended that DAC8 and MiCA introduce comprehensive privacy guidelines for cross-border data exchanges. These should encompass encryption, secure communication channels, and restricted access to sensitive data, thereby protecting user information, even when it is repurposed for other compliance areas.

Lastly, Bernt highlighted the importance of balancing transparency with privacy, suggesting that CASPs and regulators limit data collection to only essential information. Anonymization techniques, he noted, could be applied to larger datasets, thus allowing effective regulatory oversight while safeguarding individual privacy rights.

Primary Calls to Action on Privacy and Data Protection for CASPs
The primary calls to action based on the discussions are: • **Mandate Secure Reporting Tools:** Regulatory authorities should enforce the use of certified, high-security platforms for all sensitive off-chain data handling, with required encryption and access control standards.

- **Develop Data Handling Protocols:** Establish and enforce specific guidelines for managing and securing on- and off-chain data separately, with clear protective measures for any integrations.
- **Clarify Cross-border Data Privacy Standards:** Implement robust guidelines for cross-border reporting under DAC8 and CARF, ensuring secure handling protocols, restricted access, and encryption measures.
- **Adopt Privacy-Enhanced Transparency:** Regulate data collection and sharing to focus strictly on necessary information, using anonymization techniques where feasible to minimise data exposure while maintaining oversight.

We thank all participants of the Madrid roundtable for contributing to the discussion:

Adri Wischmann (IoT Netherlands), Alain Otaegui (European Banking Authority), Akli Le-Coq (Ministry of Finance), Albi Rodriguez (Garrigues), Almudena de la Mata (Blockchain Intelligence), Ana Carolina Oliveira (Venga), Carlos Escobedo (EtherNodes), and Gonzalo Navarro (ONTIER), Joaquin Sastre (Boerse Stuttgart Digital), Luiza Castro Rey (FiO Legal), Magnus Jones (EY Sweden), Marina Villalonga (Asensi Abogados), Max Bernt (Taxbit/INATBA), Mike Sadarangani (Zodia Custody), Nina Siedler (siedler legal and thinkBLOCKtank, organiser), Pedro Casanova (BBVA), Pedro Mendez de Vigo (Kraken), Reagan Cook (Taxbit), Tiburcio Sanz (Crystal), and Tommaso Astasi (BC4EU).