MICAR ROUNDTABLE EXPERT SERIES

Frankfurt

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

The ninth roundtable in this series was hosted at the Frankfurt School Blockchain Center on November 12th, 2024. We are deeply grateful to our partners and supporters who made this event possible: the European Commission, Crystal Intelligence, Frankfurt School Blockchain Center, and the Fintech Germany Award, as well as thinkBLOCKtank for their collaboration.

The Frankfurt session brought together key players from the regulatory and crypto sectors to explore essential topics related to MiCAR. Unlike previous roundtables, this session focused specifically on the intersection of MiCAR and AMLR, diving deep into their practical applications and challenges. The discussions were led by contributions from Miguel Vaz, who examined the Interoperability of the Travel Rule; Julia Lippoth, who addressed a Risk-based Approach Regarding Incoming Transfers; and Svenja Brinkmann, who discussed KYC Sharing.

This report consolidates the insights gathered during the Frankfurt 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. Interoperability of Travel Rule and Its Challenges

Miguel Vaz, Managing Director at Hauck Aufhäuser Digital Custody GmbH, presented the topic, focusing on the complexities and operational challenges associated with the implementation of the Travel Rule under MiCAR and TFR frameworks. The session explored key interoperability issues that hinder compliance and operational efficiency for CASPs within the EU and across borders.

The TFR mandates that CASPs exchange originator and beneficiary information to ensure traceability of crypto transactions, mitigating AML and CTF risks. However, interoperability challenges arise due to discrepancies in technical compatibility, compliance practices, and regulatory requirements, particularly when dealing with non-EU CASPs.

Interoperability Among EU-CASPs

Interoperability among EU-based CASPs is hindered by several factors:

- **Technical and Compliance Variations:** Differences in methods for identifying end-customers, data quality standards, and secure handling of identity data create inconsistencies.
- **Operational Costs:** CASPs are often forced to onboard multiple service providers to ensure comprehensive compliance coverage, leading to increased costs related to procurement, integration, information security, and outsourcing controls.
- **Assumptions about Licensing:** The assumption that a CASP license ensures high-quality data exchange and compliance is not explicitly stated in regulations, leading to uncertainties in data reliability.

Participants emphasized the need for a risk-based approach to data sharing, proposing reduced data exchanges in static setups with known counterparties. Instead of per-transaction data sharing, periodic monitoring could ensure compliance while minimizing operational burdens.

Interoperability with Non-EU CASPs

When interacting with non-EU CASPs, challenges intensify:

- **Regulatory Gaps:** Non-EU CASPs often lack compliance with the Travel Rule, complicating transactions and increasing risks.

- **Data Quality Concerns:** The reliability and security of identity data processing by non-EU CASPs remain a significant issue.
- **Workarounds:** Some CASPs use intermediary self-hosted wallets to manage transfers, but this approach is costly and inefficient.

Proposed solutions included introducing a Wolfsberg-style questionnaire tailored to crypto assets to ensure due diligence and compliance for non-EU counterparts. Participants also suggested clear categorization of requirements for hosted-but-non-compliant wallets to define operational and regulatory boundaries.

Alignment with eIDAS 2 and Digital Identity

The discussion also highlighted the potential of aligning Travel Rule compliance with the European Digital Identity (EUDI) wallet under eIDAS 2. The EUDI wallet, designed for secure, standardized identity verification across the EU, could provide the following benefits:

- **Standardized Identity Data Exchange:** Facilitating seamless and secure data sharing for KYC and Travel Rule requirements.
- **Privacy-Preserving Credentials:** Reducing privacy risks through verifiable credentials.
- **Trusted Identity Providers:** Leveraging eIDAS-compliant providers to confirm identity and residency, ensuring robust compliance while reducing operational complexities.

Participants noted that using eIDAS 2 trusted identity providers could streamline identity verification and reduce reliance on less secure methods, enhancing overall compliance with AML and CTF objectives.

This session underscored the urgent need for enhanced interoperability, balancing compliance requirements with operational efficiency and privacy. The participants highlighted that regulators and CASPs can address these challenges effectively by adopting risk-based approaches, aligning with digital identity frameworks, and standardizing cross-border protocols.

Primary Calls to Action for Travel Rule Interoperability

The primary calls to action based on the discussions are:

- **Implement a Risk-Based Approach:** Allow CASPs to minimize data exchanges in static setups and replace per-transaction data sharing with periodic monitoring, reducing operational burdens and privacy risks.
- **Standardize Due Diligence for Non-EU CASPs:** Introduce a Wolfsberg-style questionnaire tailored to crypto assets to ensure non-EU CASPs meet compliance standards.
- **Align Travel Rule Compliance with eIDAS 2:** Leverage the EUDI wallet and trusted identity providers to streamline identity verification and ensure secure, interoperable data exchanges.

2. Risk based approach regarding incoming crypto transfers

Julia Lippoth, Head of Compliance and MLRO at Coinbase, presented this topic, addressing the challenges posed by the stringent requirements of the TFR for CASPs. The discussion explored the operational and compliance dilemmas that CASPs face when dealing with incoming crypto transfers that lack complete TR data, particularly as CASPs must balance customer service expectations with AML/CTF obligations.

The TFR imposes stricter originator and beneficiary data requirements on crypto transactions compared to most jurisdictions globally. Article 17 allows CASPs discretion to execute, reject, return, or suspend transfers lacking complete TR data, applying a risk-sensitive approach. However, starting December 30, 2024, a significant volume of incoming transfers is expected to have incomplete or missing TR data, placing CASPs in a challenging position.

CASPs must decide how to handle these transfers without violating TR requirements while also ensuring customer satisfaction. Options such as rejecting or suspending transactions carry significant operational and reputational

risks, while executing transfers without complete data could undermine compliance efforts.

During the session, participants evaluated the options available to CASPs under Article 17:

- **Rejecting Transfers:** This is technically impractical for blockchain-based transactions, as they cannot be rejected in the same way as traditional bank wire transfers. CASPs also lack the equivalent of correspondent accounts to manage these scenarios.
- **Returning Transfers:** Returning funds to the sender's address poses risks, particularly if the originating CASP uses omnibus accounts. This could result in funds being unallocated and lost, creating further complications.
- **Suspending Transfers:** While suspension allows CASPs to seek missing information, it comes with legal risks, as holding funds indefinitely without a valid reason could undermine customer confidence. Participants agreed that suspension should be a last resort, used only in cases where there is a clear risk of money laundering or terrorist financing.
- **Executing Transfers:** This option, though preferred for minimizing customer disruption, requires robust controls to ensure compliance. Measures such as real-time data governance, automated communication with counterparty CASPs, and transaction monitoring systems (TMS) were highlighted as critical enablers for this approach.

To address these challenges, the roundtable proposed a framework that enables CASPs to execute transfers while maintaining compliance:

- **Data Governance Controls:** Implement real-time or near-real-time systems to identify missing or incomplete TR data, with the ability to escalate and report as necessary.
- **Automated Communication Systems:** Deploy systems to proactively reach out to counterparty CASPs for missing information before crediting incoming transactions.
- **TMS**: Use robust TMS to identify and flag suspicious transactions, integrating TR data into

risk-scoring models and AML/CTF compliance systems.

- **Staffed AML Function:** Ensure CASPs maintain a mature and well-trained AML team capable of embedding risk-sensitive decision-making into operational processes.

Participants also discussed the importance of balancing operational efficiency with regulatory compliance to prevent customers from switching to unregulated or less compliant platforms, which could undermine the goals of the EU's AML/CTF regime.

The Roundtable concluded that the implementation of TFR for crypto transfers presents unique challenges that require a risk-based approach tailored to the specific nature of crypto transactions. CASPs must adopt comprehensive controls, leverage technology, and maintain strong AML capabilities to manage the complexities of incoming transfers with incomplete data. It was highlighted that by executing transfers with proper safeguards, CASPs can strike a balance between customer expectations and compliance requirements, supporting the broader goals of the EU's AML/CTF framework.

The roundtable participants highlighted that to support CASPs in meeting the requirements of the TFR and broader AML/CTF obligations, regulators should incentivize the adoption of robust transaction monitoring systems, data governance frameworks, and privacy-preserving technologies such as zero-knowledge proofs. These measures will enhance compliance with TFR requirements, which mandate the exchange of originator and beneficiary information, without unnecessarily exposing sensitive data.

Additionally, clear legal frameworks for handling suspended transactions and unclaimed funds are essential to maintaining trust in regulated CASPs. Regulators should provide guidance on the conditions under which transactions can be suspended and outline the procedures for managing unclaimed funds while ensuring consumer protection.

Finally, educational efforts highlighting the benefits of regulated CASPs under the TR framework will help to discourage customers from migrating to unregulated entities, thereby strengthening the integrity of the financial system.

Primary Calls to Action for Risk-Based Approach for Incoming Crypto Transfers

The primary calls to action based on the discussions are:

- **Adoption of Robust Internal Systems by CASPs:** CASPs should implement robust transaction monitoring systems, automated communication protocols for missing data retrieval, and real-time data governance frameworks. These systems are critical for ensuring compliance with TFR and AML/CTF requirements while maintaining operational efficiency and consumer trust**.**

- **Define Clear Criteria for Addressing Incomplete TR Data:** Regulators should establish explicit criteria for CASPs to follow when dealing with incomplete Travel Rule data. These criteria should prioritize risk-sensitive decisions, allowing for the execution of transactions in cases where the AML/CTF risk is minimal. Additionally, they should mandate the implementation of robust measures, such as automated systems to retrieve missing information, while discouraging indefinite suspension or arbitrary rejection of transactions to maintain consumer trust and compliance with AML/CTF objectives.

- **Mandate Communication Standards for TR Data Resolution:** Establish secure and interoperable messaging protocols for CASPs to resolve incomplete TR data with counterparties. This will ensure consistent compliance with data quality and privacy standards across the industry.

- **Enable Risk-Based Decision-Making:** Allow CASPs to adopt a risk-sensitive approach for handling transactions with incomplete TR data. Guidelines should specify conditions under which transactions can be credited without compromising AML/CTF objectives.

3. KYC Sharing Among CASPs and Traditional Banks

The third topic, presented by Svenja Brinkmann, Senior Associate at HEUKING, addressed the complexities of collaboration between CASPs and traditional banks, with a specific focus on KYC data sharing and obligations under the TFR.

The first issue discussed was the sharing of KYC data among CASPs and their cooperation partners, such as traditional banks. CASPs often partner with banks to expand their service offerings to retail customers. In these collaborations, the CASP establishes a direct contractual relationship with the retail customer and must comply with the Money Laundering Act ("AML Act"), particularly the requirement to identify customers as per Section 10 AML Act. Under specific conditions, CASPs may use identification data collected by their cooperation partner.

However, the requirements for reusing this data under Section 17 AML Act are stringent. For example, the cooperation partner must have verified the customer's identity within the last 24 months. This limitation often renders most existing customer data unusable for CASPs, as many banks have not updated their customer records within this timeframe. Additionally, the practical implementation of "updating" identification data remains contested, with no clear consensus on whether this requires customers to re-legitimize themselves, upload and verify their IDs, or rely on previously stored, valid identification data.

The second issue concerned the applicability of the TFR. In cases where banks act as intermediaries for crypto transactions, they may not possess the necessary wallet information to transmit transaction data under the regulation. It was argued that the responsibility for transmitting transaction data should fall solely on the crypto custodian, which already fulfills the protective purpose of the regulation.

The roundtable participants highlighted that CASPs face significant challenges in leveraging identification data from their cooperation partners due to outdated requirements for data validation. The need for customer re-legitimization within 24 months creates procedural inefficiencies and increases customer friction, as most banks have not performed the required updates within this timeframe. For cooperation partners

located abroad, cross-border sharing of KYC data introduces further complications, with varying standards and legal interpretations across jurisdictions adding to the complexity.

Moreover, the role of banks under the TFR was also a central point of discussion. Banks often lack wallet-specific information for crypto transactions, making it impractical for them to comply with the regulation's data transmission requirements. Participants emphasized that crypto custodians, which directly handle the transfers, are better positioned to fulfill these obligations. This alignment would ensure compliance without imposing undue burdens on banks.

Throughout the discussion, participants stressed the need to balance regulatory compliance with practical considerations. While ensuring AML/CTF objectives are met, the regulatory framework must also provide sufficient flexibility to enable efficient collaboration between CASPs and banks. This includes creating mechanisms to reduce redundancies and streamline data-sharing processes.

The discussion highlighted the procedural inefficiencies and regulatory challenges that hinder effective collaboration between CASPs and banks. These include stringent requirements for KYC data validation, cross-border complexities, and overlapping obligations under the TFR. While the primary calls to action outline specific regulatory changes needed to address these issues, participants also emphasized operational measures for CASPs, such as improving internal KYC processes and leveraging technological solutions for compliance. The participants considered that these adjustments are critical to fostering a cooperative ecosystem that aligns with the broader objectives of the EU's AML/CTF framework.

Primary Calls to Action for KYC Sharing and Collaboration Between CASPs and Banks
The primary calls to action based on the discussions are: • **Enable Flexible KYC Data Sharing:** Regulators should issue specific guidance on the reusability of existing KYC data, particularly regarding requirements on how to update KYC data prior sharing. • **Simplify Cross-Border KYC Data Use:** Create explicit provisions within the EU regulatory framework to facilitate the cross-border sharing of KYC data among CASPs and banks, ensuring secure and consistent standards for international collaboration. • **Clarify Responsibilities Under the TFR:** Regulators should explicitly state that CASPs not directly involved in the transfer of crypto assets, such as banks transmitting orders on behalf of clients, are exempt from the obligation to transmit transaction data.

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

Alireza Siadat, Benedikt Kukacka (Crystal), Björn Weigel (Bankhaus Scheich), Dr. Nick Wittek (Jones Day), Dr. Steffen J. Härting (Deloitte), Dr. Tomasz Tomczak (Frankfurt School), Elsa Madrolle (VerifyVasp), Emir Becirbasic, Fran Romero (Cryptopocket), Irina Gorbach (Crystal), Jasper Heinrich (BaFin), Johann-Alexander Klöpper (KPMG), Julia Lippoth (Coinbase), Karen Bielau (Commerzbank), Magnus Jones (EY), Michael Heinks (Finoa), Miguel Vaz (Hauck Aufhäuser Lampe Digital Asset Custody), Miroslav Duric (Taylor Wessing), Nina Siedler, Nicole Ritter (Börse Stuttgart), Prof. Dr. Thomas Weck (Frankfurt School), Samantha Engelhardt (Risk & Regulatory Management, Börse Stuttgart), Sharon O'Donnell (Commerzbank), Svenja Brinkmann (HEUKING), Thomas Langbein (CCO Trever), and Veronique (Bitpanda).