**INTRODUCTION**

Payward Inc., d/b/a/ Kraken (“Kraken”) is pleased to respond to ESMA’s third Public Consultation on Draft Technical Standards specifying certain requirements of the Markets in Crypto-Assets (‘MiCA’) on detection and prevention of market abuse, investor protection and operational resilience.

Kraken remains committed to growing its business in the EU regulatory perimeter. Our Irish subsidiary Payward Europe Solutions Limited (‘PESL’) was granted registration as a Virtual Asset Service Provider (‘VASP’) with the Italian Organismo Agenti e Mediatori (‘OAM’) in June 2022, with the Central Bank of Ireland (‘CBI’) in April 2023, with the Bank of Spain in September 2023. Another Irish subsidiary Payward Continental Services Limited (‘PCSL’) was granted registration as a Crypto Service Provider (‘CSP’) with the Dutch Central Bank (‘DNB’) in February 2024. Kraken has also launched VASP services in Belgium through PESL. We are seeking further registrations and licences in the EU Member States as appropriate. Our licensing efforts will lead to us applying for a Crypto-Asset Service Provider (‘CASP’) licence under MiCA, when available.

Founded over 12 years ago, Kraken is one of the world’s oldest and largest global digital asset platforms. Kraken provides products and services to retail and institutional customers that support key components across the digital asset market value chain. Outside of the EU, Kraken holds several registrations, licences, authorisations and approvals including in the United States, United Kingdom, Canada, and Australia, among other developed and emerging markets.  Subject to local regulatory requirements and authorisations, Kraken’s global product and service offering includes crypto trading, investment, benchmarks, staking, banking, and others.

We welcome MiCA, as it provides legal certainty, including a clear path to licensing, and will enable the growth of our business in the EU in a manner which both protects customers and promotes confidence in the market. We welcome these technical standards and guidelines on detection and prevention of market abuse, investor protection and operational resilience as it aims to ensure customer protection while allowing innovation within the crypto-asset industry.

With regards to the topics of this consultation, Kraken is deeply committed to both safeguarding market integrity and to operational resilience. Cybersecurity has been at the forefront of Kraken’s effort ever since we were established. We are a founding member of the Crypto Information Sharing and Analysis Center (ISAC), a non-profit organisation designed to promote cybersecurity information sharing in the crypto industry. ISAC members are committed to advancing strategic objectives, including: the establishment of communication processes, the impartial and timely flow of information between stakeholders, and the continual effort to ensure crypto infrastructure is resilient.

**Summary of our response:**

* **The scope of PPAETs should not extend the scope of MiCA Level 1**: We agree in general with the scope of CASPs being considered as persons professionally arranging or executing transactions (“PPAETs”). However, miners and/or validators are not in scope of MiCA - Level 1 and as such they should not be considered in scope of PPAETs.
* **The requirement to monitor certain DLT aspects such as MEV should be exluded:** We note that the proposed requirements for PPAETs, including CASPs, to have processes in place to monitor and report on “other aspects of the functioning of the distributed ledger technology (DLT)”, such as maximal extractable value (MEV), are not proportionate and should be **excluded from the draft rules**.
  + Majority of CASPs such as trading platforms operate in a **centralised** off-chain environment, where MEV does not occur. Exchanges such as Kraken maintain a central limit order-book and as such have a greater control over the orders, and can apply market abuse rules as appropriate.
  + MEV is a **feature of a decentralised system**. MEV can **contribute to market efficiency** by allowing more accurate pricing across DeFi markets and allowing users to buy assets with tighter spreads across various decentralised protocols.
  + Despite these benefits, MEV can at times also lead to negative behaviours. However, CASPs, validators, and DeFi dapps are **not privy to any exclusive off- or on-chain data required to execute MEV** and so detection of market abuse would be very challenging.
  + Instead of monitoring, the blockchain community is actively working to **mitigate the negative externalities of MEV**, e.g. by providing free tools to protect Ethereum transactions from frontrunning and sandwich attacks.
  + **From a technology perspective**, applying any blanket approach to this requirement would also be difficult given that **different chains have different mechanisms and nuances**.

We would be pleased to discuss any points or questions raised in further detail.

Please see our detailed responses on the guidelines in the separate attachment.

-- End --