December 14, 2023

European Securities and Markets Authority
ESMA
201-203 rue de Bercy
CS 80910
75589 Paris Cedex 12
France

By Online Submission

Dear Sir/Madam

Re: Public Comment on the Second Consultation on the Technical Standards specifying certain requirements of Markets in Crypto Assets Regulation (**MiCA**)

Fireblocks appreciates the opportunity to provide comments on the Second Consultation on the Technical Standards specifying certain requirements of Markets in Crypto Assets Regulation ("**Consultation Paper**"). Fireblocks is committed to the mission of enabling businesses to easily and securely support virtual assets. As such, we welcome ESMA's invitation for comments on its draft regulatory technical standards (**RTS**) and implementing technical standards (**ITS**).

We set out, in this submission, our response to Question 17 of the Consultation Paper.

About Fireblocks

Fireblocks Ltd is an Israeli company with various subsidiaries around the world (together, "**Fireblocks**"). Since 2019, Fireblocks has been providing institutional customers with an enterprise-grade platform that facilitates their self-custodial storage, transfer, and management of virtual assets (the "**Platform**"). The Platform is provided to customers as a software-as-a-service offering.

The Platform enables customers to create secure environments known as "vaults" for the holding of virtual assets. Within these vaults, customers are able to designate "sub-vaults" to segregate their virtual asset holdings. These sub-vaults function as virtual asset wallets. Customers can also transfer virtual assets out of the vault to any specified location. The Platform allows customers to streamline the management of their virtual asset holdings with third-party exchanges, over-the-counter dealers, counterparties, and traditional "control" custodians by making these holdings visible to the customer and allowing their secure administration within a single software environment. There are currently more than 1,700 institutions using our Platform and Fireblocks is widely considered one of the most secure custodial software solutions available.

To date, the Platform has obtained the following certifications:

- SOCII Type2
- ISO 27001
- ISO 27017
- ISO 27018
- Cryptocurrency Security Standard (CCSS) Qualified Service Provider Level 3 certification by the Cryptocurrency Certification Consortium (C4)

Response to Question 17 of the Consultation Paper - "Q17: Are there other organisational measures to be considered for specific CASP services?"

In responding to this Question 17, we focus on organizational measures supporting business continuity and disaster recovery, which we understand to be a focus of the Consultation Paper. While we acknowledge that MiCA requires CASPs to implement appropriate procedures to ensure resilient and secure information and communication technology (ICT) systems and to establish general business continuity, recovery and response plans, we also believe that there are specific organizational measures for CASPs to consider that specifically rely on third party software providers for their digital asset custody services. We believe that because these Custody Technology Service Providers ("CTSPs") are mission critical service providers to CASPs, organizational measures should include rules and standards for CASPs to consider in selecting CTSPs. ESMA should consider the following elements for best practices with respect to CASPs' business continuity, disaster recovery and resolvability plans when using CTSPs:

- *Service Level Agreements.* CTSPs should offer their CASP customers SLAs that, at a minimum, conform to the CTSPs' own enterprise policies and procedures regarding availability targets and service recoverability. CTSPs should be expected to target high availability and implement failover architecture. ESMA has articulated that it wants to avoid introducing any ICT specific requirements for CASPs but targeting high availability and requiring the implementation of failover architecture for the CTSPs on which they rely would align with establishing best practices for digital asset custody service providers.

- *Incidence Response*. In line with Article 4 of the draft RTS, CASPs should adopt policies and procedures for the identification and timely response to service disruptions. These policies and procedures should also extend to the CASP's use of CTSPs. At a minimum, such policies and procedures should define the operational roles and responsibilities for the CASP's personnel, their CTSP counterparts, and include a specific action plan for addressing foreseeable outages by CTSPs. The CTSPs should provide the same to the CASP to rely upon. This is touched upon in Article 2 of the draft RTS, requiring CASPs to employ personnel capable of discharging the duties allocated to them, but the additional specificity in also requiring appropriate policies and procedures for incident responses and clarity on operational roles and responsibilities of the CTSPs that CASPs

rely on will ensure that the designated personnel can discharge those duties appropriately during the heightened calamity of an actual incident response.

- *Third Party Dependency Management*. Pursuant to Article 4 of the draft RTS, CASPs should perform a risk assessment and diligence on their own critical vendors and functions as part of their continuity and recovery preparation. This undoubtedly should include CTSPs on which CASPs rely for their digital asset custody services. The CASPs' review and risk assessment should be incorporated into the periodic review process of the CASPs' business continuity policy but should also incorporate the CTSP's own risk assessment.

- *Business Continuity and Disaster Recovery*. Article 4 of the draft RTS requires CASPs to adopt plans and conduct exercises reasonably designed to ensure business continuity and service recoverability plans in case of severe operational disruptions. Such plans should be expected to include:
    - Multiple, specified risk scenarios and targeted recovery times.
    - Periodic validation and updating requirements.
    - Contingency plans for critical vendor outages.

  We acknowledge that ESMA has addressed some of these points in Articles 4 and 5 of the draft RTS, with the obligations for periodic testing of the business continuity plan, to be reviewed by the CASP's management body, and subject to an independent assessment (either internal or third party vendor).

- *Management Change Procedures.* CTSPs should provide technical methods and procedures to their CASP customers to enable them to safely migrate platform access and authorization rights from one employee to another, including blocking, retiring and rolling access to private keys from old employees to new employees.

- *Backup and recovery key management*. ESMA should consider ways to incent market participants to adopt prudent backup and recovery key management practices for digital asset custody services and/or step in to create additional market infrastructure. ESMA should consider private and public options, including the following:
    - Require CASP's backup keys to be held in dedicated entities under escrow or escrow-like arrangements.
        - However, there are very few service providers qualified to do this today. ESMA should consider that such a rule, if adopted, may result in concentrations of systemic risk in only a few market participants.
    - Establish a government sponsored utility for the purpose of safekeeping backup keys for digital asset custody services.
        - While this solution also creates concentration risk, governments may be better suited to the task of systemic risk management than the private sector. Such an entity could be funded by an assessment on industry

participants and operated without profit motive, like a member-owned clearinghouse or public utility.

- Depending on the nature of the digital asset custody solution, ESMA should consider requiring CTSPs that provide digital asset custody services to CASPs to deploy technology to allow CASPs to verify that backup keys have been stored correctly.

- *Resolution Plans.* CASPs should be expected to use CTSPs who engage in resolution planning exercises such that the CTSP could be placed into insolvency proceedings with a clear plan for the transfer of CASP customer key material. ESMA should consider whether periodic approval of such plans and the publication of ratings would enhance the integrity of the market and confidence of market participants. Plans may include:
  - An assessment of operations, services and key material related to securing and accessing customer wallets;
  - A wind-down plan, including plans for the transfer of any of the identified critical operations, services or key material; and
  - Periodic audit and/or supervisory review.

****

We look forward to further discussions with the ESMA on the points raised in this submission. Please do not hesitate to reach out to John McCarthy (john.mccarthy@fireblocks.com). We would be delighted to work with the ESMA further as it continues to seek public input in developing its policy recommendations.

Sincerely,

John McCarthy
General Counsel