Response to ESMA's 3rd Consultation Package on MiCAR covering draft technical standards and guidelines specifying certain requirements on detection and prevention of market abuse, investor protection and operational resilience

The Crypto Council for Innovation (CCI) welcomes the opportunity to submit comments on ESMA's third consultation package ('ESMA CP') under the Markets in Crypto-assets Regulation (MiCAR). Our comments, summarised below and detailed in subsequent pages, cover the draft technical standards/guidelines on: detecting and reporting suspected market abuse; advice and portfolio management; procedures and policies for crypto-asset transfer services; and the maintenance of systems and security access protocols.

We recommend that ESMA makes the following changes to its proposals in the CP:

'Personal Scope' of MiCA's Market Abuse Regime

- Market participants who primarily secure and operate a blockchain (e.g., miners and validators) and who do not arrange or execute transactions, should not be treated as persons professionally arranging or executing transactions (PPAETs).
- Other market participants such as custodians and administrators, should only be treated as PPAETs if their operating model gives them the capacity to observe and report suspicious and potentially abusive market behaviour.
- The distinct market abuse rules in MiCA and MaR that apply to different categories of market participant should be respected and not conflated or cumulatively applied to PPAETs and to CASPs operating a trading platform.
- Decentralised protocols should be explicitly excluded from the scope of MiCA's market abuse regime to reflect differences in the approach that is necessary to prevent and detect abusive behaviour in centralised and decentralised systems.

Treatment and Reporting of Maximum Extractable Value Strategies

- Maximum Extractable Value (MEV) strategies should not be implicitly categorised as abusive behaviour by default and CSAPs should not be required to submit STORs for all MEV activity.
- Consistent with MiCA, CASPs should only be required to monitor activity on their own systems to determine, based on specific circumstances and due consideration of fairness, whether MEV strategies raise a reasonable suspicion of abusive behaviour and therefore should be reported (e.g., consistent with the Proof of Stake Alliance's Fair Market Principles for MEV).

Suspicious Transaction or Order Reporting

- References to 'validators of transactions in a distributed ledger system' should be removed from suspicious transaction or order reports (STORs) templates consistent with the exclusion of miners and validators from the scope of MiCA's market abuse regime (see above recommendation).
- The requirement to report publicly available information in STORs should be removed and a taxonomy should be developed with parameters and naming conventions to improve the efficiency of reporting.
- IP addresses and other geo-location information should only be collected and reported on STORs if this supports rather than counters accurate analysis of the location of suspicious activity.

Suitability Assessment for Advice and Portfolio Management Services

- The suitability assessment for advice and portfolio management services should be adapted from MiFID II to reflect fundamental differences between crypto-assets and financial instruments such as the 'inputs' (e.g., consensus mechanisms) for assessing crypto-assets against investor sustainability preferences.
- Existing approaches to sustainability reporting should not be extended to decentralised protocols to avoid undermining the fundamental nature of decentralised systems.

Procedures, policies and rights of clients for crypto-asset transfer services

- CASPs should be required to provide clients with information and conditions related to transfer services for crypto assets in electronic format rather than a durable medium.
- The obligation for a CASP to provide the clients with information on the amount of any charges for the crypto-asset transfer payable by the client should be clarified as relating only to charges known to the CASP.
- The requirement to disclose the means of communication agreed between parties for the transmission of information or notifications related to the crypto-asset transfer service should be clarified to exclude those technical requirements not relevant to a client making a transaction decision.
- The interaction with the Transfer of Funds Regulation (TOFR) of proposed requirements for a CASP to provide information to its client at the time of transfer, and for a CASP to develop risk-based policies and procedures for the refusal or rejection of transfer requests, should be clarified.
- References to 'off-DLT transfers' should be clarified as capturing 'on-chain transactions'.
- Higher-level information on transfers should be provided to clients with signposting to more granular information to ensure clients who are less familiar with crypto-asset transfer services are not overwhelmed.

Systems and Security Access Protocols

- References to 'offerors' in the context of the 'systems' that must be maintained under MiCA, should be clarified as excluding decentralised protocols on the basis that ESMA has identified that they do not pose risks to stability of the crypto-asset market.

Arrangements, systems & procedures for detecting & reporting suspected market abuse in crypto-assets

ESMA has proposed draft technical standards (Section 7.2.1, ESMA CP) under its mandate in Article 92(2), MiCAR covering:

- arrangements, systems and procedures for CASPs to prevent and detect market abuse;
- a reporting template for suspicious transaction and order reports (STORs); and
- coordination procedures between competent authorities for detecting and sanctioning market abuse.

Q1: Do you agree with ESMA's analysis on the personal scope of Article 92 of MiCA? Are there other types of entities in the crypto-asset markets that should be considered as a PPAET (e.g. miners/validators)? Do you believe that CASPs providing custody and administration of crypto-assets on behalf of clients should also be considered as PPAETs for the purpose of this RTS? Please elaborate.

ESMA should treat Brokers[1] and exchanges[2] as persons professionally arranging or executing transactions (PPAETs). Market participants who primarily secure and operate a blockchain (e.g., miners and validators) and who do not arrange or execute transactions should not be treated as PPAETs. ESMA should determine that the operating model of market participants, such as custodians and administrators, gives them the capacity to observe and report suspicious and potentially abusive behaviour before treating them as PPAETs.

Treatment of brokers, exchanges, miners and validators

Brokers and exchanges are likely to have the most direct vantage point to observe and subsequently report suspicious and potentially abusive behaviour. However, market participants such as miners and validators who primarily secure and operate a blockchain, do not arrange or execute transactions and therefore may not have an effective vantage point to identify suspicious and potential abuse behaviour nor the information to report such behaviour. ESMA should align its definition of a PPAET with the Market Abuse Regulation[3]. Extending the PPAET definition to cover market participants such as miners and validators who primarily secure and operate a blockchain may reduce innovation of decentralised networks, threaten data and network security, and counter sustainability efforts by disincentivizing some consensus mechanisms over others.

Treatment of custodians and administrators

ESMA should not consider custodians and administrators as PPAETs by default. The operating model of a custodian or administrator, including whether it has direct or indirect end-client contact, will determine whether it is party to information that:

i. enables it identify and report suspicious and potentially abusive behaviour;
ii. could be used by actors (e.g., employees) for insider dealing or market manipulation.

[1] e.g., providing MiCA services such as receiving, transmitting or executing orders and providing fiat-to-crypto exchange,
[2] e.g., operating a trading platform
[3] Article 3(28) of Regulation (EU) No 596/2014 (i.e., MAR) defines a PPAET as a person professionally engaged in the reception and transmission of orders for, or in the execution of transactions in, financial instruments.

In line with the approach that ESMA is proposing for personal account dealing (paragraph 38, ESMA CP) and the STOR template, ESMA should identify the 'capacity' of an entity to identify and report suspicious and potentially abusive behaviour to determine whether it should be considered a PPAET.

Q2: Do you agree with the proposed elements that should constitute appropriate arrangements, systems and procedures to detect and prevent market abuse? If not, please specify the article of the draft RTS and elaborate.

We recommend the following changes to ESMA's proposals for preventing and detecting market abuse, discussed in more detail below:

- ESMA should not conflate the MiCA and MAR market abuse frameworks[4] and instead respect the different obligations imposed on market operators and PPAETs by each regime;
- ESMA should also not cumulatively apply MiCA's market abuse rules to PPAETs[5] and CASPs operating a trading platform[6] and instead only apply the distinct obligations for each category of market participant (Paragraph 16, ESMA CP).
- ESMA should formally clarify that decentralised protocols are excluded from the scope of MiCA's market abuse regime, to reflect differences in the approach that is necessary to prevent and detect abusive behaviour in centralised and decentralised systems.[7]
- ESMA should not implicitly categorise Maximum Extractable Value (MEV) strategies as being abusive behaviour by default and therefore should not require CSAPs to submit STORs for all MEV activity. Consistent with MiCA, ESMA should only require CASPs to monitor activity on their own systems to determine, based on specific circumstances and due consideration of fairness, whether such strategies raise a reasonable suspicion of abusive behaviour and therefore should be reported.

Application of MiCA's Market Abuse Rules

CASPs and other market participants have an important collective role to detect and prevent market abuse, including in partnership with NCAs through the submission of STORs. The role market participants can and should play depends on various factors including the nature of their activities, their vantage point over orders and transactions, the information they have access to, and their capacity to report suspected abusive behaviour.

MiCA obliges those CASPs which operate a trading platform for crypto-assets[8] and those which are PPAETs[9] to prevent and detect suspected market abuse. However, MiCA only requires CASPs which are PPAETs to submit STORs when:

[4] Article 16 (MAR) and Article 92, MiCA
[5] Article 92, MiCA
[6] Article 76(7)(g), MiCA
[7] Recital 22, MiCAR descopes crypto-asset services that are provided in a fully decentralised manner without an intermediary.
[8] Article 76(7)(g), MiCA
[9] Article 92, MiCA

- they have reasonable suspicion about transactions and orders, including any cancellation or modification thereof, and other aspects of the functioning of the distributed ledger technology (DLT) such as the consensus mechanism; and
- there might be circumstances that indicate that market abuse has been committed, is being committed or is likely to be committed.

The distinction in obligations under MiCA between CASPs which operate a trading platform for crypto-assets and PPAETs mirrors the approach in MAR, which distinguishes between the role of market operators to prevent and detect suspected market abuse[10] and the role that PPAETs (e.g., brokers) can play in detecting and reporting transactions where they have a reasonable suspicion of market abuse.[11]

We do not agree with ESMA's approach to cumulatively apply MiCA's market abuse obligations in a broad brush manner to CASPs which operate a trading platform for crypto-assets and to PPAETs (Paragraph 16, ESMA CP). Given ESMA's suggestion that custodians and administrators could be considered as PPAETs, this would appear to imply that all CASPs together with miners and validators (under ESMA's proposals to treat them as PPAETs) would be subject to the full MiCA market abuse regime, including monitoring the functioning of the DLT and its consensus mechanism. We respectfully request that ESMA reconsiders its proposed interpretation of MiCA's market abuse rules on the basis that this:

- ignores the distinctions drawn in MiCA between CASPs which operate a trading platform for crypto-assets and PPAETs; and
- is unlikely to uncover abusive behaviour commensurate with the cost and resource required for implementation, given that a significant volume of trading and of price formation occurs off-chain (i.e., requiring 'internal' monitoring by centralised market operators).

Explicit Exclusion Of Decentralised Protocols From MiCA's Market Abuse Regime

ESMA should formally clarify that decentralised protocols are excluded from MiCA's market abuse regime, consistent with the exclusion of crypto-asset services provided in a decentralised manner from the scope of MiCA.[12] Detecting and preventing market abuse in decentralised systems requires a different approach to centralised ones.

Traditional approaches to detecting and preventing market abuse may be ineffective for decentralised systems and reduce their utility, as decentralisation can eliminate information asymmetry and therefore inside information by avoiding reliance on the management of an enterprise. Instead, market abuse mitigations such as token lockups may be more effective while preserving the utility of decentralisation. Such an approach reflects that decentralisation is the key determinant of risk for a given crypto asset, as the transparent nature of many public blockchains enables holders of assets to find relevant information on-chain to assess value and trade on a level playing field. This is distinct from centralised crypot-assets which derive their value from the efforts of the management of an enterprise. As such, the market abuse related risks to users in the primary and secondary market will depend on whether the asset is centralised or decentralised.

[10] Article 16(1), MAR
[11] Article 16(2), MAR
[12] Recital 22, MiCAR descopes crypto-asset services that are provided in a fully decentralised manner without an intermediary.

Maximum Extractable Value

We respectfully request that ESMA reconsider its implicit definition of Maximum Extractable Value (MEV) strategies as being abusive behaviour by default. CASPs should not be required to report STORs for all MEV activity.

MEV is a broad-based term for a range of order sequencing activities. Research has shown that MEV strategies can have positive or negative effects on users. On the one hand, MEV can provide benefits,[13] including informing blockchain design, applications and supporting infrastructure and protocol security, and creating financial incentives to improve price and trading execution efficiency.[14] On the other hand, MEV has also been identified as adversely impacting users where conflicts of interest are not managed, including exploiting information asymmetries of users.

Given the variability of MEV strategies and their implications for users, and consistent with MiCA, CASPs should only be required to monitor activity on their own systems and only be obliged to submit STORs in respect of MEV strategies based on the following:

- when they become aware of suspected abusive behaviour from having put in place appropriate arrangements for systems and procedures for monitoring and detecting market abuse on their own systems;[15]
- having analysed the circumstances indicating that market abuse has been committed, is being committee or is likely to be committed; and
- after due consideration of the 'fairness' of the MEV strategy i.e., balancing the benefits of MEV with maintaining a fair and secure blockchain network (e.g., consistent with the Proof of Stake Alliance's Fair Market Principles for MEV).

We acknowledge the challenges for ESMA in constructing an approach to MEV which prevents abusive behaviour while maintaining flexibility in order-sequencing to enable the development and optimisation of crypto markets. We also note that supervisors and other market participants have access to publicly available information (e.g., transactions on public blockchains) and therefore will have at least as good a vantage point from which to surveil markets as CASPs.

Q3: Do you agree with the proposed STOR template as presented in the Annex of the RTS?

We support ESMA's overall approach to developing the proposed STOR template, but do not agree that market participants who primarily secure and operate a blockchain (e.g., miners and validators) and who do not arrange or execute transactions should be deemed PPAETs and therefore be required to submit STORs (see our response to question 1.) We therefore respectfully request that ESMA removes the references in Section 5 of the proposed template to 'validators of transactions in a distributed ledger system.'

[13] *See* UK Financial Conduct Authority, Review of Maximal Extractable Value & Blockchain Oracles, February 2024, available at https://www.fca.org.uk/publication/research-notes/research-note-review-and-maximal-extractable-value-blockchain-oracles.pdf
[14] *See* Crypto Council for Innovation: What is MEV?, available at https://cryptoforinnovation.org/what-is-mev/
[15] Article 92, MiCA

We caution ESMA against requiring too much information in the STOR template to avoid hampering efficient reporting. We recommend that ESMA seeks to eliminate requirements to report publicly available information such as the description of the functioning of the DLT.

We also encourage ESMA to develop further guidance, including Q&A, to support CASPs and other PPAETs when completing and submitting STORs. For instance, we recommend that ESMA provides examples of the supporting documentation and materials, including templates, that should be provided with the STOR (i.e., in Section 6).

Q4: Is there any parameter or naming convention that in your view should be modified to facilitate the identification of suspicious orders/transactions/behaviours involving crypto-assets?

We recommend that ESMA develops a taxonomy to define the parameters and naming conventions for the submission of crypto-asset related STOR templates. For instance, a 'transaction types' taxonomy could include 'swap', 'transfer' and a 'suspicious behaviours' taxonomy could include 'rug pulls', 'oracle manipulation' and 'pump-and-dump'.

Q5: In Section II of the Annex, would the concept of 'location' be applicable to a distributed ledger? For instance, would the IP address of miners/validator nodes in the network be useful in a context where it can be masked through VPNs?

We support the rationale for collecting information on the time and location of the suspected activity on STORs but highlight the complexity of applying the concept of "location" for DLT as, due its decentralised nature, pinpointing a single physical location for an order is challenging.

Collecting IP addresses may be helpful in some instances but the potential for obfuscation through VPNs and other anonymisation techniques will reduce reliability for determining the actual location of the suspicious activity and may make data analysis counterproductive.

Aspects of the suitability requirements applicable to the provision of advice and portfolio management in crypto-assets and the format of the periodic statement

ESMA has proposed guidelines (Section 5, ESMA CP) under its mandate in Article 81(5), MiCAR covering various aspects of the assessment of a client's knowledge and competence to determine the suitability of a crypto-asset investment and the format of the periodic portfolio management statement.

Q8: Do you agree with ESMA's approach regarding consistency between the MiCA and MiFID II suitability regimes? If you think that the two regimes should diverge, where and for which reasons?

We broadly support ESMA's overall approach to developing guidelines for the suitability assessment. We agree that for common elements between financial instruments and crypto-assets (e.g., investment risk) there is merit in basing the suitability assessment under MiCA on the existing MiFID II framework. In some areas,

however, the fundamentally different nature of crypto-assets and financial instruments raises different considerations for suitability and warrant a different approach.

We do not agree with the direct copy across of the MiFID II obligations to collect a client's sustainability preferences. While the overarching objective of collecting these preferences is to identify products (including investments) which have sustainability features which align a client's sustainability preferences, some 'inputs' for this assessment are different for crypto-assets compared to other investments. In the context of an investment product, a client may be concerned with the minimum proportion of their portfolio that are in investments with particular sustainability features e.g., an investment fund with an 'impact' strategy. In the case of crypto-assets, as acknowledged by MiCAR,[16] inputs can include the consensus mechanism used for the validation of blockchain transactions. Given the differences, we recommend that ESMA revises its proposed guidelines to acknowledge that the collection of a client's sustainability preferences should take account of the relevant 'inputs' for crypto-assets.

Furthermore, as set out in our response to ESMA's second MiCA consultation,[17] ESMA should avoid extending its existing sustainability reporting approach (e.g., under SFDR) to decentralised protocols as this is untenable and undesirable. We acknowledge the challenges in developing an approach to sustainability data that reflects the globally distributed nature of decentralised protocols. However, given the distributed, open-source nature of decentralised protocols and the absence of centralised intermediaries capable of providing data on protocols' behalf, imposing traditional approaches could undermine the fundamental nature of decentralised systems. We look forward to providing input to further consultations as policy approaches in this area develop.

Procedures and policies, including the rights of clients in the context of transfer services for crypto-assets

MiCAR requires CASPs providing transfer services for crypto-assets[18] on behalf of clients to conclude an agreement with their clients to specify their duties and their responsibilities.[19] MiCAR also specifies the minimum content of the agreement.

ESMA has proposed draft guidelines (Section 7.2.3, ESMA CP) under its mandate in Article 82(2), MiCAR covering the procedures and policies, including the rights of clients, in the context of transfer services for crypto-assets.

Q11: Do you agree with the approach taken by ESMA in the draft guidelines for cryptoasset service providers providing transfer services for crypto-assets on behalf of clients as regards procedures and policies, including the rights of clients? Please also state the reasons for your answer.

We broadly support ESMA's overall approach to developing the draft guidelines. In particular, we commend ESMA for recalling that while certain crypto-asset transfer services share similarities with payment services, crypto-assets are treated as distinct from 'funds' in a payment services context (e.g., under PSD2). ESMA has

[16] Recital 7, MiCAR

[17] *See* 'Sustainability Indicators' section, of CCI's Response to ESMA's consultation (second batch) under MiCA, December 2023, available at https://media.cryptoforinnovation.org/2023/12/CCI-response-to-ESMA-MiCA-consultation-second-batch-.docx.pdf

[18] 'Providing transfer services for crypto-assets on behalf of clients' means providing services of transfer, on behalf of a natural or legal person, of crypto-assets from one distributed ledger address or account to another (Article 3(1)(26), MiCAR)

[19] Article 82(1), MiCAR

correctly given due regard to ensuring consistent with the guidelines and the transfer of funds regulation (e.g., for EMTs which are treated as crypto-assets rather than 'funds').

We recommend that ESMA makes following changes to the proposed guidelines:

- Amend the proposal for a CASP to provide the client with information and conditions related to the transfer services for crypto-assets in a durable medium and instead require this to be provided in an electronic format (i.e., a durable medium other than paper as per Article 4(62a), MiFID II). Clients engaging in crypto-asset transfers can reasonably be expected to be familiar and comfortable with information in electronic form and there is no need for other durable mediums (e.g., paper) to be explicitly permitted for the provision of information and conditions by CASPs to clients.

- Clarify that the obligation for a CASP to provide the client with information on the amount of any charges for the crypto-asset transfer payable by the client and, where applicable, a breakdown of the amounts of such charges, relates only to charges that are known to the CASP (paragraph 16, Guideline 2). Upon receipt of an instruction to transfer crypto-assets but before execution, a CASP may not be aware of other charges levied by third parties (e.g., levied by an intermediary or the receiving CASP).

- Clarify what is meant by the requirement to disclose 'the means of communication, including the technical requirements for the client's equipment and software, agreed between the parties for the transmission of information or notifications related to the crypto-asset transfer service' (p90, ESMA CP). Messaging on transfer services may occur within the client's online account opened with the CASP, for instance via a web-based or mobile application and therefore specific technical requirements for the client's equipment and software may not be relevant to a client making a transaction decision.

- Clarify the interaction of the proposed requirement for a CASP to provide information to its client at the time of a transfer, with the information that the client would have initially provided to the CASP under the Transfer of Funds Regulation (i.e., do CASPs need to report back information to clients that they have already provided).

- Clarify how the requirements for the development of risk-based policies and procedures for the refusal or rejection of transfer requests due to Transfer of Funds Regulation (TOFR) requirements (i.e., travel rule) or other issues, interact with the TOFR and related guidance being prepared by the EBA (i.e., do the guidelines under the TOFR take precedence over those in MiCA or vice versa.)

Q12: Do you think that the draft guidelines address sufficiently the risks for clients related to on- and off-DLT crypto-asset transfers? Please justify your answer.

We respectfully request that ESMA clarifies its reference to 'off-DLT transfers' as capturing on-chain transfers of crypto-assets from one distributed ledger address or account to another, consistent with MiCA's definition of transfer services.[20]

[20] Article 3(26), MiCA

We broadly support ESMA's approach to providing information on individual transfers for crypto-assets (Guideline 2). ESMA's proposal to provide clients with brief and standardised information on the irreversibility of transfers and the charges for transfers seem to strike the right balance between high-level and detailed information.

We are concerned that ESMA's proposals to also provide clients with more granular information before a transfer, such as the number of block confirmations needed for a transfer to be irreversible, may overwhelm clients who are less familiar with crypto-asset transfer services (e.g. retail clients). Providing clients with higher-level information, such as a summary of the costs applicable to a transfer service and the key risks, while signposting to them where more granular information is available may engender greater client engagement if they are able to better 'see the wood from the trees'.

Maintenance of systems and security access protocols in conformity with appropriate Union standards

ESMA has proposed guidelines (section 7.2.4, CP) under its mandate in Article 14(1)(d), MiCAR for offerors and persons seeking admission to trading of crypto assets that are not ARTs or EMTs to maintain all of their systems and security access protocols in conformity with appropriate Union standards.

Q14. Do you support ESMA's interpretation of the term, 'systems' in the mandate? If not, please explain your understanding of the term (and provide examples if possible).

We agree with ESMA's proposal to interpret 'systems' under its MiCA mandate as referring to ICT systems. This interpretation is consistent with the policy intention to capture "offerors and persons seeking admission to trading" who ESMA has identified do not "pose risks to the stability of the crypto-asset market nor to investors " on the same scale as CASPs.' We would welcome clarity from ESMA that its reference to offerors is not intended to capture decentralised protocols.

Q16. Do you agree with the inclusion of minimal administrative arrangements in Guideline 2 (i.e., no reference to implementing a risk management framework)? If no, please explain whether you would consider either fewer or more administrative arrangements appropriate.

We agree with ESMA's proposal to focus on administrative arrangements rather than mandating risk management and governance requirements. We noted that ESMA recalls that Guideline 2 lists many recognisable aspects of a standard risk management framework.

Q17. Do you support the inclusion of Guideline 5 on 'cryptographic key management'? Do you consider cryptographic keys relevant as either a 'system' or a 'security access protocol'? Is this guideline fit for purpose (i.e., can cryptographic keys be 'replaced' as implied in paragraph 29)?

We agree with ESMA's proposal that the offeror or persons seeking admission to trading have designated adequate staff for managing the specific ICT and physical risks associated with the use of cryptographic keys.