25 March 2024
ESMA75-453128700-1012
ESMA74-449133380-434

-

Reply form

to the Consultation Paper on certain requirements of the Markets in Crypto Assets Regulation (MiCA) on detection and prevention of market abuse, investor protection and operational resilience – third consultation paper

-

Responding to this paper

ESMA invites comments on all matters in this consultation paper and in particular on the specific questions. Comments are most helpful if they:

- respond to the question stated;
- indicate the specific question to which the comment relates;
- contain a clear rationale; and
- describe any alternatives ESMA should consider.

ESMA will consider all comments received by **25 June 2024.**

Instructions

In order to facilitate analysis of responses to the Consultation Paper, respondents are requested to follow the below steps when preparing and submitting their response:

1. Insert your responses to the questions in the Consultation Paper in the present response form.
2. Use this form and send your responses in Word format (**pdf documents will not be considered except for annexes**);
3. Please do not remove tags of the type <ESMA_QUESTION _MIC4_1>. Your response to each question has to be framed by the two tags corresponding to the question.
4. If you do not wish to respond to a given question, please do not delete it but simply leave the text "TYPE YOUR TEXT HERE" between the tags.
5. When you have drafted your response, name your response form according to the following convention: ESMA_MIC4_nameofrespondent_RESPONSEFORM. For example, for a respondent named ABCD, the response form would be entitled ESMA_MIC4_ABCD_RESPONSEFORM.
6. Upload the form containing your responses, **in Word format**, to ESMA's website (www.esma.europa.eu under the heading "Your input – Open Consultations" -> Consultation Paper on guidelines on conditions and criteria for the classification of crypto-assets as financial instruments").

Publication of responses

All contributions received will be published following the close of the consultation, unless you request otherwise. Please clearly and prominently indicate in your submission any part you do not wish to be publically disclosed. A standard confidentiality statement in an email message will not be treated as a request for non-disclosure. A confidential response may be requested from us in accordance with ESMA's rules on access to documents. We may consult you if we receive such a request. Any decision we make not to disclose the response is reviewable by ESMA's Board of Appeal and the European Ombudsman.

Data protection

Information on data protection can be found at www.esma.europa.eu under the heading Legal Notice.

Who should read this paper

- All interested stakeholders are invited to respond to this consultation paper. In particular, ESMA invites crypto-assets issuers, crypto-asset service providers and financial entities dealing with crypto-assets as well as all stakeholders that have an interest in crypto-assets.

General information about respondent

Name of the company / organisation	*Global Blockchain Business Council (GBBC)*
Activity	Non-financial Counterparty
Are you representing an association?	☒
Country/Region	Europe

About us:

GBBC is the largest leading industry association for the blockchain technology and digital assets community. Launched in Davos in 2017, GBBC is a Swiss-based non-profit, with more than 500 institutional members, and 301 Ambassadors across 117 jurisdictions and disciplines. The organisation is dedicated to furthering adoption of blockchain technology by convening regulators, business leaders, and global changemakers to foster collaboration and advance dialogue to create more secure, equitable, and functional societies.

Executive summary:

GBBC welcomes ESMA's work in establishing robust guidelines, standards and procedures which contribute to investor protection, market confidence and prevent market abuse.

This consultation response focuses on the guidelines and technical standards proposed by ESMA. Our analysis addresses several key issues, including the scope of Article 92, identifying and defining PPAETs, and considering whether miners, validators, and CASPs should be encompassed by the regulation.

GBBC highlights the importance of appropriate systems and procedures which can help prevent market abuse, especially through the integration of both on-chain and off-chain data for monitoring. GBBC members suggest enhancements to the STOR template, enabling it to capture a wider range of transaction types and suspicious activities which are unique to crypto-assets.

Additionally, we examine the feasibility of using advanced geolocation techniques beyond IP addresses and discuss the costs and benefits of implementing the proposed standards.

In this response, we outline GBBC's support for aligning MiCA with MiFID II suitability regimes to ensure consistency and investor protection, at the same time recognizing the need for tailored guidelines to address the specific risks of crypto-assets.

We also advocate for amendments to the draft guidelines to enhance risk disclosures, security measures, and investor education.

Our response stresses the necessity of effective cross-border regulatory coordination and adherence to global standards ensuring that EU regulations maintain market integrity and investor confidence.

Questions

1. **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_QUESTION_MIC4_1>

ESMA provides a detailed analysis of the personal scope of Article 92 of the MiCA regulation, which identifies entities that should be considered as PPAETs. ESMA's analysis aims to ensure that the entities classified under Article 92 are those that have a significant impact on the crypto-asset markets and the broader financial ecosystem. This includes ensuring transparency, integrity, and investor protection within the market. The criteria for identifying PPAETs typically involve evaluating their roles, influence, and the nature of their activities within the crypto-asset ecosystem.

MiCA, under Article 92, has a very broad definition of a CASP and identifies a long list of activities that are carried out by a CASP. These include:

- Crypto-asset service providers (CASPs) operating trading platforms.
- CASPs providing services such as:
    - Receiving or transmitting orders for crypto-assets on behalf of clients.
    - Executing crypto-asset orders for clients.
    - Managing crypto-asset portfolios.
    - Exchanging crypto-assets for funds or other crypto-assets.
- Professionals dealing in crypto-assets on their own account or as part of a business should also be considered PPAETs, especially if they have dedicated trading desks.

While there is no definition of a PPAET in MICA, "MAR defines a PPAET under Article 3(28) as "a person professionally engaged in the reception and transmission of orders for, or in the execution of transactions in, financial instruments". As stated in the Consultation Paper, this concept was addressed by an ESMA Q&A (Question 6), making clear that the definition of PPAETs should be read in a broad sense, encompassing buy-side firms, proprietary traders, DEA providers and non-financial firms that trade on their own account as part of their business activities". Furthermore, MICA defines "reception and transmission of orders for crypto-assets on behalf of clients'" as "the reception from a person of an order to purchase or sell one or more crypto-assets or to subscribe for one or more crypto-assets and the transmission of that order to a third party for execution".

A CASP carrying out several of these activities should certainly be considered a PPAET. However, it is also the case that a CASP carrying out other activities in this list, such as purely custody and administrative activities, should not be considered a PPAET. As ESMA points out in paragraph 14, MiCA requires that a PPAET "have arrangements, systems and procedures to prevent, detect and report to NCAs possible market abuse cases". To prevent market abuse effectively, appropriate systems and controls should be in place to monitor orders, transactions, and other activities, tailored to the nature and scale of the business. This includes assessing the risk posed by the activities of the PPAETs or their clients, directly linked to known market abuse and crypto-specific manipulation typologies. This is a requirement that would be impossible for a CASP carrying out purely custody and administrative activities to meet and would be a barrier to the provision of such CASP services.

For a CASP, it will be critical to have an understanding of the precise list of CASP activities that will result in a CASP being treated as a PPAET. The consultation paper, notably in paragraph 37 on page 13, and in Recital 2 on page 41, does not give a precise list. In their final form, the RTS should provide clarity on this point.

Miners and validators play a crucial role in maintaining the integrity and security of blockchain networks. They validate transactions and add new blocks to the blockchain, ensuring the decentralised nature of these networks but they are not "intermediaries". Despite their pivotal role, they should "not" be considered PPAETs. In other words, MiCA was initially designed to regulate crypto-asset issuers and CASPs, focusing on aspects such as issuance, trading, custody, and market manipulation. Validators and miners, while crucial to blockchain networks, do not typically engage in activities directly covered by MiCA's initial scope, such as offering crypto-assets to the public or providing custody services. In fact, validators and miners are fundamentally different from CASPs in their roles and functions. Their primary responsibility is to maintain network security and transaction integrity, rather than directly engaging with end-users or financial markets. Including them under MiCA could blur the lines between network infrastructure roles, and financial service roles. Furthermore, expanding MiCA to cover validators and miners might be seen as regulatory overreach, potentially stifling innovation and imposing undue compliance burdens on entities that were not the primary focus of the regulation. This could lead to unintended consequences, such as driving these activities out of the EU to more favourable jurisdictions. On the other hand, validators and miners are critical to the operation and security of blockchain networks. Their activities have significant implications for the stability and integrity of these networks. In fact, ensuring that validators and miners operate under certain standards could enhance overall trust in blockchain networks, aligning with MiCA's objectives of investor protection and market integrity. In conclusion, the

balance between fostering innovation and ensuring robust regulatory oversight will be key in determining the appropriate scope of MiCA and ESMA's role in this evolving landscape.

In addition to that, the inclusion of validators and miners as PPAETs could have several potential implications under the Anti-Money Laundering Regulations (AMLR) and the Transfer of Funds Regulation (TFR). Validators and miners may be subject to more rigorous scrutiny by financial regulators to ensure compliance with AMLR and TFR standards. They might need to implement Know Your Customer (KYC) and Anti-Money Laundering (AML) procedures to identify and monitor their users and transaction flows. They could be required to report suspicious activities and transactions to the relevant authorities, increasing their administrative burden. Miners and validators would need to conduct enhanced due diligence on transactions to prevent illicit activities, which could slow down transaction processing and increase operational costs. Implementation of compliance mechanisms might necessitate changes to their infrastructure, such as integrating KYC/AML tools and ensuring secure data storage. In fact, stricter regulations might stifle innovation by imposing rigid compliance frameworks on new technologies and practices. Last but not least, implementing KYC/AML measures might raise privacy concerns among users who value the pseudonymous nature of blockchain transactions. Blockchains extend beyond financial transactions and are utilised by unregulated industries due to their ability to tokenize any asset. Validators ensure the security and integrity of blockchains by adding transactions to the distributed ledger, akin to how internet routers forward IP packets without inspecting them. In Western countries, IP scanning on the public internet is seen as a privacy violation. Similarly, the introduction of transaction scanning on public blockchains could be deemed a violation of values and rights protected under EU privacy laws.

To assess if validators, miners or other players in the network could qualify as PPAET, it is important to highlight that each decentralised blockchain network's native process for processing, ordering, and finalising user transactions and intents can widely differ. Each network, whether abiding by a Proof-of-Work (PoW), Proof-of-Stake (PoS), or other consensus algorithms, may have unique characteristics in accomplishing the above-mentioned process of settling user transactions and intents on-chain. For example, Ethereum has developed a unique market structure that outsources the arranging aspect of pending transaction processing to actors that sit outside of the protocol. Ethereum protocol's ultimate end goal of Proposer-Builder Separation (PBS) has been temporarily implemented through Flashbot's middleware MEV-Boost, which allows Ethereum validators to outsource the block-building (i.e., transaction arranging) component of their responsibilities on the execution layer. Around 90% of Ethereum validators have elected to connect to the 'builder market' via MEV-Boost. Within that builder market exists an ecosystem of actors that help advance the arranging of pending transactions to an ultimate end state of a fully ordered block that can be delivered to the validator for proposal to the network.

The primary actors within this ecosystem at the moment are searchers, builders, and relays. Given their current roles in the ecosystem, it is our opinion that searchers and builders should be subject to rules preventing them from market manipulation or fraudulent activity, e.g., front running based on insider information, pertaining to private order flow from users. The distinction between public and private transactions is nuanced, but for the purposes of this response, we can say that public transactions are those which land in the public mem pool and can be "read" by any node on the network without encryption or time delay. On the other hand, users may protect their transactions from becoming public by submitting them to private RPC nodes, which will forward them to select builders. Those nodes may delay broadcasting those transactions for a short period of time (to assess the MEV extraction opportunity). By most definitions, private order flow constitutes a significant percentage of the overall order flow on the Ethereum network today. On the other hand, searcher and builder activity on public order flow/transactions requires more research, in our opinion, before regulators should definitively ascribe abuse to certain types of MEV extraction (and thus before regulators should impose monitoring and reporting obligations on searcher and builder interaction with public transactions in the block-building ecosystem).

Validators in this value chain receive an already constructed block of pending transactions from the relay that was previously arranged by the builder. At this point, there are economic mechanisms that greatly disincentivize the validator from attempting to rearrange the ordering of pending transactions within the block that was provided to them. Furthermore, the Validators must operate within the bounds of the deterministic smart contracts that govern the protocol (e.g., block gas limits, block time). For these reasons, the validator will in almost all cases propose the block as received by the relay to the network for validation. Assuming the validator's behaviour is consistent with this normal standard (contrasted to the exploitative activity of unbundling private transactions as highlighted in the recent indictment by the DOJ), the validator will not be involved in (re)arranging the pending transactions. Therefore, under this part of the definition, the validator should not qualify as a PPAET.

Evaluating the qualification of a Validator as a PPAET under the second part of the definition noted above, pertaining to the execution of transactions, hinges upon the explicit definition of 'execution' as it relates to pending transactions evolving into confirmed transactions. In traditional finance, the execution of a transaction is performed, typically, by a venue with some obligations around execution quality (price, timeliness). On Ethereum, most of those traditional obligations have been outsourced to other actors, as noted above. Furthermore, on Ethereum, a pending transaction included within a block of transactions and proposed to the network by a validator is only considered finalised and settled after it has undergone a certain number of network confirmations, which occur after the point in time when the validator performs their obligations of proposing a block to the network. The likelihood for validators to manipulate the

market and thus harm users as part of this confirmation process is unlikely, for technical and financial reasons.

In many ways, the validator acts similarly to a telecommunications infrastructure provider rather than a broker with fiduciary obligations. Here, it is worth pointing out that the FATF and IOSCO have qualified stakers-validators as infrastructure providers as opposed to financial service providers. We agree with this view as it pertains to validators on the Ethereum network. Nevertheless, we believe validators are still able to (and should) mitigate risks associated with on-chain market abuse or exploits as well as other financial crime risks such as sanctions/terrorism financing/money laundering. As is well known, certain builders filter out OFAC-sanctioned transactions and validators have the technical discretion/capability to accept transactions from only certain builders/relays.

On other blockchain networks, validators may play the role of both arranging pending transactions into a block and proposing that block to the network. Therefore, validators on networks which don't primarily outsource the block-building responsibilities of a validator may potentially qualify as a PPAET on a case-by-case basis.

We agree with ESMA's provisions stipulated in Article 91, which includes examples of common manipulation typologies. Drawing from GBBC's member experience of a crypto-native trade surveillance and transaction monitoring platform for crypto-assets, we have also identified several other abusive behaviours that express crypto's unique challenges.

Because the crypto-asset ecosystem is built on an entirely different market infrastructure, with significant retail involvement, assets without centralised issuers, and a proliferation of centralised and decentralised venues for trading, market manipulation can involve some novel mechanisms. Challenges unique to crypto assets include manipulations that take place cross on- and off-chain, cross-venue (including centralised venues and decentralised exchanges), pre-chain (i.e., before the transaction is confirmed on-chain as part of the proof of stake block-building process), or in relation to smart-contract integrity. These behaviours may already be covered by existing legislative frameworks which broadly prohibit manipulative and fraudulent practices but the novelty of some of these manipulation typologies could require different parameters and detection methods.

Regarding staking rewards, MiCA specifies that staking rewards linked to the maintenance of distributed ledgers are excluded from public offer rules but still fall under its regulatory scope. However, EU Directive 2023/2226 amending Directive 2011/16/EU on administrative cooperation in the field of taxation curiously includes staking along with lending as crypto-asset services, despite MiCA not explicitly categorising them as such. We believe that clarity is greatly needed for all actors to understand their responsibilities.

ESMA's Draft of the Technical standards addresses the risks posed by MEV (Miner/Maximal Extractable Value). This includes monitoring the consensus mechanisms in distributed ledger technology to prevent market abuse, such as transaction front-running by miners or validators. We believe that ESMA may also consider evaluating conflicts of interest for service providers involved in MEV activities to maintain market integrity, especially between searchers, builders, relays, validators and the entities that operate them; as well as financial crime risks that all those different actors may face. Indeed, establishing integrity-driven, safe and secure network protocols is crucial for on-chain market integrity and customer protection, fostering trust, mitigating risks, and ensuring transaction reliability. We believe that implementing robust pre-chain financial crime compliance controls such as detecting wallets and transactions linked to illicit activities (before they are validated) is essential to keep the system safe and secure and prevent its abuse by bad actors. Pre-chain risk controls address a broad range of illicit activities, including market abuse and smart contract exploits. To prevent crypto crimes, network participants should consider employing risk management tools aimed to surface, identify, and attributing potential risky or malicious behaviour occurring within the block-building process.

Particularly, smart contract scams involve the exploitation of trust through fraudulent or malicious smart contract code, design or investment schemes. While smart contract scams are a form of fraud, we emphasize the importance of specifically identifying them as a unique offence within the crypto landscape due to their prevalence and potential for prevention. This distinction enables targeted measures to address and mitigate these specific scams. We believe that to adequately safeguard crypto asset investors, it is crucial to develop regulatory frameworks that require CASPs to proactively block hard-coded smart contract scams at the protocol level. Because these attacks occur on-chain, there should be tools that can achieve this through automated scam detection, auditing, and metrics on each token using data fine-tuned from the thousands of tokens examined each day. By implementing standards for code audits, CASPs can combat smart contract scams effectively, and foster a safer ecosystem for all participants involved.

<ESMA_QUESTION_MIC4_1>

2. **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.**

<ESMA_QUESTION_MIC4_2>

GBBC agrees with the proposed elements that constitute appropriate arrangements, including real-time monitoring, alert generation, audit trails, transmission of information to the regulator,

adequate expertise, and delegating investigation to experts, among others. We also agree that CASPs should require **appropriate arrangements**, systems and procedures, **based on the nature, scale and complexity of the CASP's business** to effectively mitigate market abuse risks. As crypto-asset markets continue to evolve and expand, CASPs play a critical role in detecting and preventing fraudulent activities and contributing to confidence in the markets. Thus, real-time, alert-generating market surveillance that allows effective and timely detection of market abuse is essential.

It is equally important for CASPs to have in place systems that holistically monitor for both on and off-chain manipulation. The combination of on-chain and off-chain data enables a more comprehensive analysis of user behaviour and transaction patterns. By analysing both sets of data, CASPs can better identify suspicious activities, including wash trading, front-running, and spoofing. It is important to emphasise that AML transaction monitoring and trade surveillance systems should not operate in silos. As the Japan Financial Services Authority indicated in its July 2023 paper titled "*Report of FSA's Joint Research on Analyzing Decentralized Financial System using On-Chain and Off-Chain Data*," despite its transparency and ease of tracing, on-chain data alone does not suffice to capture all the necessary information for regulatory compliance and market integrity, such as user identity or source of funds. It also does not include the vast majority of crypto trading volume which is traded on off-chain, centralised platforms. By incorporating off-chain data, including user KYC (Know Your Customer) information, transaction history, and fiat currency conversion records, along with centralised orderbook data, CASPs and regulators have a more comprehensive view of the investment journey and can detect market abuse throughout the digital asset lifecycle, cross-asset and cross venue. This more effectively monitors potential risks associated with illicit activities and ensures compliance with anti-money laundering (AML) and counter-terrorism financing (CTF) regulations. Moreover, the combination of on and off-chain data facilitates faster and more accurate detection and response to potential risks and instances of market abuse. Swift identification of anomalies or suspicious patterns allows for prompt intervention and mitigation of fraudulent activities. Such responsiveness plays a pivotal role in maintaining market integrity and fostering investor confidence in the crypto ecosystem.

Additionally, cross-venue manipulation often involves price manipulation that directly impacts on-chain liquidity pools and DEXs, as well as some centralised platforms. The execution of on-chain manipulations frequently occurs off-chain, underscoring the critical importance of scrutinising unusual volume or price movements across both on-chain and off-chain data sources. This example underscores the need for cross-venue market surveillance. It is thus key for the regulators to identify and set in place mechanisms that would allow information sharing of suspected market abuse behaviours between CASPS, as well as between NCAs.

We also believe that there should be standards developed around data generation and retention to ensure sufficient transaction details such as timestamps and prices are being recorded and are available after the fact.

Trade surveillance risk scoring should be integrated into the overall risk scoring of CASPs' customers. The risk scoring analysis should be integrally part of any trade surveillance systems at a transactions level and customer level, including alerts generated on the customers over time, risk concentration, comparison of customer's behaviour with his historical data, benchmark with peers and market conditions.

To streamline STOR filing, monitoring systems should allow PPAETs to automatically generate standard and custom reports and extend copies to the regulators on specific incidents, trends, specific accounts or specific risk concentrations. It is well known that regulatory actions resulting from compliance deficiencies are often the result ***not*** of lacking trade surveillance or transaction monitoring, but of failing to appropriately calibrate parameters for alerting, thus overwhelming compliance officers with false positives that cannot be appropriately dispositioned. This has a downstream impact on flooding regulators, in some cases, with a high volume of low-signal suspicious transaction reports. Therefore, it is imperative that trade surveillance systems enable CASPs (and regulators who may use the systems for supervision) to surgically calibrate algorithm parameters relevant to the particular asset and its liquidity profile, the customer segment (e.g., retail vs. institutional), and the type of trade activity (e.g., market-making). These features are necessary and when implemented correctly, considerably increase market surveillance efficiency.

Finally, all trade surveillance systems should include an audit trail and reporting capabilities, record keeping and in-depth analyses of transaction histories. The solution should also allow auditable backtesting, which will facilitate the response to subpoenas or regulatory investigations. With such functionalities in place, PPAETs will be fully prepared and equipped to demonstrate their capacity to prevent and detect market abuse.

Overall, GBBC believes that the implementation of appropriate market surveillance tools in the crypto ecosystem can foster markets that are safe and even more transparent compared to traditional finance. Through comprehensive surveillance that covers the entire ecosystem, a deeper understanding of market dynamics can be attained, mitigating the risks associated with manipulative practices and fostering fairer and more efficient markets.

<ESMA_QUESTION_MIC4_2>

3. **Do you agree with the proposed STOR template as presented in the Annex of the RTS?**

<ESMA_QUESTION_MIC4_3>

The STOR template entails some of the data points that might not be feasible for the market participants to provide, particularly concerning aspects of the distributed ledger technology (DLT) like consensus mechanisms, which some firms may not have the technological capacity to access. We support the view that some of the data fields are required only if they are applicable and known, such as NIN, date of birth, LEI of the CASP, account number, relationship with the issuer, type of activity of the trading desk, etc. As for, the description of the order, transaction or suspicious behaviour related to the functioning of the distributed ledger technology, we believe that "the type of order" and "the way it was placed" are possible to report, while "the person that actually received the order" and" the means by which the order is transmitted" might be difficult (or practically impossible) to access. Therefore, for these data elements, it may be advisable to include the condition "if applicable and known". As for full client address, size of portfolio, date of business relationship started, and employment information of the underlying client - these data points are not necessarily required on a continuous basis for market abuse purposes, and may create an additional burden for reporting suspicious behaviour in the context of market abuse.

<ESMA_QUESTION_MIC4_3>

4. **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?**

<ESMA_QUESTION_MIC4_4>

Transaction Type can be expanded:

1. Expanded Options for Transaction type: Swap," "Transfer," and "Smart Contract Interaction." This reflects the diverse range of transaction types common in the crypto-asset market.

   Definitions:

   - **Swap -** An exchange of one crypto asset for another, typically occurring on a decentralised exchange (DEX) platform without the need for a central intermediary.
   - **Transfer -** The movement of a crypto asset from one wallet to another.
   - **Smart Contract Interaction -** Transactions that involve executing the terms of a smart contract on a blockchain.

2. Non-Standard Transactions: to ensure all types of transactions are accurately reported and analysed we suggest leaving the list of the transaction types open, allowing to specify the type in another field (for example DEX trade). The template will be better equipped to handle the diverse and evolving nature of the crypto-asset market.

In order to better capture the wide range of suspicious activities specific to the crypto-asset market, GBBC members propose to expand the list of suspicious behaviours to include:

1. Wash Trading: Artificially inflating trading volumes to create a false impression of market activity.
2. Pump-and-Dump Schemes: Coordinated efforts to inflate the price of an asset before selling off at the peak.
3. Spoofing: Placing fake orders to manipulate prices and create misleading market conditions.
4. Rug Pulls: Developers abandoning a project and absconding with investor funds.
5. Oracle Manipulation: Manipulating the data sources used by smart contracts to exploit vulnerabilities.
6. Front-Running: Exploiting advanced knowledge of upcoming transactions to make a profit, typically by placing orders ahead of the known transaction.
7. Phishing Attacks: Using deceptive emails, messages, or websites to trick individuals into revealing private keys or other sensitive information.
8. Sybil Attacks: Creating multiple fake identities to gain disproportionate influence or control over a network or platform.
9. Layering: Conducting a series of complex transactions to disguise the origin and ownership of funds, often used in money laundering.
10. Transaction Reordering: Reordering transactions within a block to exploit discrepancies in timing and execution for financial gain.
11. Whale Manipulation: Large holders (whales) make significant trades to manipulate market prices for profit.
12. Exit Scams: Operators of an exchange or platform abruptly shut down and abscond with users' funds.
13. Dusting Attacks: Sending tiny amounts of crypto to multiple addresses to break the privacy of wallet holders by tracking their transactions.
14. Token Hijacking: Unauthorised creation or issuance of tokens to manipulate supply and control market dynamics.
15. Consensus Mechanism Exploitation: Manipulating the consensus process of a blockchain network to gain an unfair advantage or disrupt network operations.

<ESMA_QUESTION_MIC4_4>

5. **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?**

<ESMA_QUESTION_MIC4_5>

While the concept of "location" can be applicable to a distributed ledger, it comes with significant challenges due to the decentralised and anonymized nature of the network. IP addresses of miners/validator nodes might offer some utility, but their usefulness is limited by the potential for masking through VPNs and other tools. In regulatory contexts, it may be more effective to use a combination of data points and analytical techniques to infer the location and understand the network's geographical distribution.

That said, one of GBBC's members conducted a comprehensive study comparing the effectiveness of using location indicators in the context of Distributed Ledger Technology (DLT). The goal was to identify more reliable methods for geolocation beyond IP address node tracking, which can serve as additional geolocation evidence but be masked through VPNs. The study explored alternative techniques that provide better insights for law enforcement and regulatory purposes.

The research identified several innovative approaches that do not rely on IP addresses. These methods offer enhanced geolocation capabilities and are applicable across various blockchain networks, not just Bitcoin.

Temporal Analysis:

- Transaction Timestamps: By aggregating and visualising transaction timestamps, we can create a heatmap that suggests potential geographic locations (e.g., countries) based on activity patterns.
- Example Analysis: For instance, analysing transaction activity during specific times and days can infer potential time zones and working patterns of the users.

IP Address Aggregation:

- Cluster-Level Data: Aggregating IP address data per cluster can indicate the most popular nodes a user interacts with, providing insights into service providers and geographic zones.

Enhanced Visualisation:

- Heatmaps and Activity Charts: We propose using heatmaps to visualise transaction activity, offering soft geolocation that avoids the pitfalls of relying solely on IP addresses. This method presents data in an intuitive way, allowing it to detect patterns more easily.

Additional Propositions:

Node Analysis:

- Service Correlation: Blockchain analytic tools could analyse which nodes are most common with specific services and make this data available for the regulator

Node Reputation Score:

- Risk Factor: Developing a 'node reputation score' could serve as a risk factor for various client verticals. This score would consider the reliability and trustworthiness of nodes based on their behaviour and interactions. However, given the weaknesses in geolocation, this remains a supplementary indicator rather than a definitive measure.

Proposed Solutions:

We recommend integrating the following features into the product to enhance geolocation and activity profiling:

Geolocation Heatmaps:

- Visualise aggregated transaction timestamps to infer geographic regions. Provide a more accurate and user-friendly method to understand activity patterns.

IP Address Clustering:

- Show the most common IP addresses used per cluster, useful for identifying service providers and geographic zones Support temporal analysis by correlating IP data with transaction activity.

Comprehensive Activity Profiling:

- Combine temporal and IP analysis to assess working hours and active days. Enrich user experience by offering insights into operational patterns, which are critical for law enforcement and regulatory actions.

We are prepared to share detailed results and methodologies upon request. By integrating these enhanced geolocation techniques, we can improve the identification and tracking of suspicious activities in the crypto-asset market, providing a significant advantage over current methods.

<ESMA_QUESTION_MIC4_5>

6. **Is there any other element or information relevant to crypto-asset markets that in your view should be included in the template? Please explain.**

<ESMA_QUESTION_MIC4_6>

GBBC encourages ESMA to consider collecting data on categories which can help address the unique characteristics and challenges of crypto-assets and their functionality within the market and trades. Proposed Additional Fields for STOR:

1. Wallet Addresses involved in the transaction to help link activities across different transactions and identify suspicious patterns.
2. Suspicious Behaviour Indicators such as wash trading, pump-and-dump schemes, spoofing, rug pulls, oracle manipulation, front-running, phishing attacks, Sybil attacks, layering, transaction reordering, whale manipulation, exit scams, dusting attacks, token hijacking, and consensus mechanism exploitation.
3. Contextual Information such as prevailing market conditions, significant news events, or other external factors influencing trading behaviour.
4. Social Media Information and Activity associated with the crypto-asset or participants. This can help identify coordinated efforts to manipulate market sentiment or price.

We believe that by incorporating these additional fields, the STOR template would be better suited to address the unique aspects of the crypto-asset market. At the same time, GBBC highlights that because the template requires a comprehensive data set, it might be necessary to review how this data corresponds with the GDPR requirements and how it interacts with the cross-border regulatory coordination.

<ESMA_QUESTION_MIC4_6>

7. **Please provide information about the estimated costs and benefits of the proposed technical standard, in particular in relation to the arrangements, systems and procedures to prevent and detect market abuse.**

<ESMA_QUESTION_MIC4_7>

While the initial and ongoing costs of implementing the proposed technical standard to prevent and detect market abuse are significant, the benefits in terms of enhanced market integrity, regulatory compliance, operational efficiency, and long-term competitive advantage are substantial. Firms should weigh these costs and benefits carefully, considering not only the financial impact but also the strategic advantages of fostering a fair and trustworthy market environment. Companies will need to invest in advanced surveillance systems, data analytics

tools, and blockchain monitoring software. Additional costs would include training and hiring qualified staff, such as risk managers and compliance personnel specialised in digital assets. The cost for these can vary widely depending on the size and complexity of the operations, but for medium to large firms, this could range from €50,000 to €500,000.

At the same time, given the advancement of technology and the introduction of modern, cost-efficient risk monitoring and infrastructure, such costs might not be as burdensome compared to traditional finance. For example, crypto-native market surveillance technologies provide free data access, unlike traditional legacy systems.

<ESMA_QUESTION_MIC4_7>

8. **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?**

<ESMA_QUESTION_MIC4_8>

ESMA's approach to aligning the MiCA regulation with the MiFID II suitability regimes aims to create consistency in investor protection across traditional financial instruments and crypto-assets. This consistency can simplify compliance for firms operating in both sectors and ensure a similar level of protection for investors regardless of the type of asset they are dealing with. In fact, aligning MiCA with MiFID II ensures that investors in crypto-assets receive a similar level of protection as those in traditional financial markets. This includes suitability assessments to ensure that investment products are appropriate for the investor's risk profile and investment objectives. Consistency between the two regimes provides regulatory clarity for firms, reducing the complexity and costs associated with compliance. Firms can apply a single set of principles across different types of assets, streamlining their operations and compliance efforts. On the other hand, crypto-assets are generally more volatile and speculative compared to traditional financial instruments. This inherent risk profile means that the suitability assessments might need to incorporate additional criteria or weightings specific to the unique risks of crypto-assets.

In spite of all that, consistency between MiCA and MiFID II suitability regimes offers several benefits, there are valid reasons to consider divergences in specific areas to account for the unique characteristics of crypto-assets. These divergences should aim to enhance investor protection by addressing the particular risks and challenges associated with crypto-assets, while still maintaining the overarching goals of regulatory clarity, market integrity, and investor confidence. By striking the right balance between consistency and tailored regulations, ESMA can ensure a robust framework that effectively governs both traditional financial instruments and the evolving crypto-asset market. However, it is important to consider the potential

competitive disadvantages faced by European startups compared to their Asian and American counterparts, who may operate under less stringent regulatory pressures and require less financial and regulatory expertise at the outset. Therefore, when harmonising MiFID II and MiCA, it is essential to address the risk of European startups relocating to other jurisdictions due to these disparities. The harmonisation can provide an opportunity to leverage the regulatory landscape and promote the ecosystem's growth within the EU.

<ESMA_QUESTION_MIC4_8>

9. **Do you think that the draft guidelines should be amended to better-fit crypto-assets and the relevant crypto-asset services? In which regard? Please justify your answer.**

<ESMA_QUESTION_MIC4_9>

We agree that the draft guidelines should be amended to better-fit crypto-assets and the relevant crypto-asset services. Crypto assets typically exhibit much higher volatility compared to traditional financial instruments. Enhanced risk disclosures are necessary to ensure investors understand the potential for significant price swings. Additionally, crypto-assets operate on complex technologies like blockchain. Investors need to understand these technologies to make informed decisions. The crypto market is less mature and more prone to market manipulation compared to traditional financial markets. Enhanced due diligence and monitoring are necessary to address these risks. Crypto-assets attract a younger and often less experienced investor base. Enhanced suitability criteria and educational requirements can help protect these investors from making uninformed decisions. Guidelines should ensure that crypto-asset service providers implement strong security measures to protect investors' assets.

The nature of crypto transactions can make them attractive for illicit activities. Enhanced AML and CTF measures are crucial to prevent abuse. Ensuring that crypto-asset service providers adhere to stringent AML and CTF standards will help integrate these assets into the broader financial system while maintaining regulatory compliance.

Amending the draft guidelines to better fit the specific characteristics of crypto-assets and their services is essential for creating a robust regulatory framework. Such amendments will help mitigate the unique risks associated with crypto-assets, enhance investor protection, and promote market integrity. Tailored guidelines will also ensure that the regulatory approach remains adaptive and responsive to the evolving nature of the crypto market.

<ESMA_QUESTION_MIC4_9>

10. **Do you agree with the approach followed by ESMA regarding periodic statements provided in relation to portfolio management of crypto-assets?**

<ESMA_QUESTION_MIC4_10>

GBBC welcomes ESMA's approach to periodic statements for the portfolio management of crypto-assets as an important step towards ensuring transparency, accountability, and investor protection in the crypto market. By requiring comprehensive, clear, and frequent updates, ESMA can help investors stay informed and make better decisions. However, considering the unique aspects of crypto-assets, there is room for refinement and further improvements. Enhancements such as more frequent reporting, inclusion of technological risks, tailored performance metrics, and investor education components could further improve the effectiveness of these statements and better serve the needs of crypto-asset investors.

<ESMA_QUESTION_MIC4_10>

11. **Do you agree with the approach taken by ESMA in the draft guidelines for crypto-asset 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.**

<ESMA_QUESTION_MIC4_11>

GBBC supports upfront disclosure of key service information such as procedures, policies and rights to end-clients. This allows clients to evaluate the risks, costs, and legal terms of crypto-asset transfers, and determine if service levels match their risk appetite and investment goals. As crypto-asset transfer volumes increase and investor types broaden, service levels will increasingly need to match those found in traditional markets where upfront disclosure is consistently applied.

<ESMA_QUESTION_MIC4_11>

12. **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.**

<ESMA_QUESTION_MIC4_12>

On-DLT transfers typically involve transactions directly recorded on a blockchain. Risks such as unauthorised access to private keys, smart contract vulnerabilities, and 51% attacks need to be considered. In addition to that, smart contracts used in on-DLT transfers may contain coding errors or vulnerabilities that could result in financial losses. On the other hand, off-DLT transfers often involve third-party custodians or intermediaries. Risks include custodial mismanagement, insolvency of custodial entities, and counterparty risks. Off-DLT transfers

may be subject to regulatory scrutiny and compliance requirements, including AML/KYC regulations and financial licensing obligations.

Whether the draft guidelines sufficiently address the risks related to on- and off-DLT crypto-asset transfers depends on the comprehensiveness and effectiveness of the measures outlined. If the guidelines include robust security standards, transaction verification procedures, smart contract auditing requirements, and custodial safeguards for both on- and off-DLT transfers, they would likely be deemed sufficient in addressing the associated risks. However, if the guidelines are lacking in these areas or fail to provide clear guidance on regulatory compliance obligations, custodial standards, and risk mitigation measures, they may be considered insufficient in adequately addressing the risks for clients related to on- and off-DLT crypto-asset transfers.

<ESMA_QUESTION_MIC4_12>

13. **Are there any additional comments that you would like to raise and/or information that you would like to provide, for example, on whether other relevant points or clients' rights should be considered?**

<ESMA_QUESTION_MIC4_13>

1. Clients' rights to privacy should be carefully considered, especially concerning the collection, storage, and use of personal data in compliance with data protection regulations like GDPR. Clients should have access to clear and understandable information about the risks, fees, and terms associated with crypto-asset services to make informed decisions.

   Promoting investor education and awareness initiatives can empower clients to better understand crypto assets, their risks, and how to safeguard their investments. For these reasons, regulatory frameworks should provide clarity on the legal status of crypto-assets and the obligations of service providers, reducing uncertainty and fostering market confidence.

2. With respect to the coordination procedures between national competent authorities for the detection and sanctioning of cross-border market abuse situations, we agree with ESMA that the establishment of detailed procedures for NCAs to exchange information, coordinate investigations, and report on enforcement activities is essential. This ensures consistent supervisory efforts within the EU and promotes transparency among authorities. Similarly, IOSCO emphasizes the necessity of international cooperation frameworks that facilitate

information sharing and enforcement assistance across jurisdictions. Both entities recognize the importance of collaboration in maintaining market integrity enhancing regulatory oversight and prioritising cross-border cooperation to address market abuse effectively.

<ESMA_QUESTION_MIC4_13>

14. **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).**

<ESMA_QUESTION_MIC4_14>

"Systems" typically refer to the technical infrastructure, platforms, and networks used by financial market participants to execute transactions, manage data, and provide services. Examples include trading platforms, order management systems, risk management systems, market surveillance tools, and reporting systems.

<ESMA_QUESTION_MIC4_14>

15. **Are there other 'appropriate Union standards' beyond those identified in the consultation paper that you consider relevant for this mandate? If yes, please list them and provide a rationale for why they would be relevant.**

<ESMA_QUESTION_MIC4_15>

To begin with, the International Organization of Securities Commissions (IOSCO) Principles for securities regulation set out international standards for promoting fair, efficient, and transparent markets. Adherence to IOSCO Principles can help ensure that regulatory frameworks for financial markets, including systems and processes overseen by ESMA, are aligned with global best practices.

Furthermore, compliance with EU directives and regulations on data protection, such as the General Data Protection Regulation (GDPR), is crucial for ensuring the privacy and security of personal data processed by financial institutions. Adherence to GDPR principles can help mitigate risks related to data breaches and enhance consumer trust. The Financial Action Task Force (FATF) Recommendations provide international standards for combating money laundering, terrorist financing, and other illicit activities. Compliance with FATF Recommendations can help ensure that financial institutions have robust AML/CFT measures in place to prevent misuse of their systems and services for illicit purposes.

<ESMA_QUESTION_MIC4_15>

16. **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.**

<ESMA_QUESTION_MIC4_16>

The inclusion of minimal administrative arrangements in Guideline 2, without specific reference to implementing a risk management framework, may not provide sufficient guidance for ensuring robust risk management practices within financial institutions. A risk management framework provides a structured approach for identifying, assessing, and mitigating risks across various aspects of an organisation's operations, including systems, processes, and activities. (A.Lanotte, "Keys to Maintaining Trust and Credibility With Stakeholders" TNI, Feb.2024). Without a risk management framework, financial institutions may struggle to comprehensively identify and assess the diverse risks they face, including operational, technological, market, and regulatory risks. On the other hand, a well-defined risk management framework enables financial institutions to proactively identify potential risks and take appropriate measures to mitigate them before they materialise. In fact, by implementing effective risk controls and monitoring mechanisms, institutions can reduce the likelihood and impact of adverse events on their operations and stakeholders. While minimal administrative arrangements may streamline regulatory compliance, omitting specific references to implementing a risk management framework in Guideline 2 may undermine effective risk management practices within financial institutions.

<ESMA_QUESTION_MIC4_16>

17. **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 of the draft guidelines)?**

<ESMA_QUESTION_MIC4_17>

Guideline 5 on cryptographic key management is both relevant and fit for purpose in the context of regulating crypto-asset service providers. Cryptographic keys are essential components of systems and security access protocols in the crypto-asset ecosystem, and effective key management is critical for safeguarding assets and maintaining trust in financial markets. By providing guidance on cryptographic key management practices, including key generation, storage, usage, and replacement, Guideline 5 helps ensure that financial institutions have the necessary controls and procedures in place to protect cryptographic keys and mitigate

associated risks. In fact, cryptographic keys play a critical role in securing digital assets, authenticating transactions, and protecting sensitive information.

<ESMA_QUESTION_MIC4_17>