SUBMITTED VIA WEB FORM TO: https://www.esma.europa.eu/

To whom it may concern,

Re: European Securities & Markets Authority (ESMA) Consultation Paper on draft technical standards and guidelines specifying 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

About Global Digital Finance (GDF)

GDF is the leading global members association advocating and accelerating the adoption of best practices for crypto and digital assets. GDF's mission is to promote and facilitate greater adoption of market standards for digital assets through the development of best practices and governance standards by convening industry, policymakers, and regulators.

The input to this response has been curated through a series of member discussions and roundtables, and GDF is grateful to its members who have taken part.

As always, GDF remains at your disposal for any further questions or clarifications you may have, and we would welcome a meeting with you to further discuss these matters in more detail with our members.

Yours faithfully,
Elise Soucie - Director of Global Policy & Regulatory Affairs - GDF

Response to the Consultation Report: Executive Summary

GDF convened its Markets in Crypto-Assets (MiCA) Working Group to analyse the European Securities & Markets Authority (ESMA) Consultation Paper on draft technical standards and guidelines specifying certain requirements of the Markets in Crypto Assets Regulation (MiCA) on detection and prevention of market abuse, investor protection and operational resilience. Please note that as this response was developed in collaboration with GDF members, as well as community partners, that portions of our response may be similar or verbatim to individual member responses. In particular, GDF was pleased to collaborate on this response with the ACI Financial Markets Association and are grateful for their contributions.

Overall, GDF is supportive of the aim of the proposals made in the third Consultation Paper and of ESMA's intent of providing much needed clarity to the market. We appreciate the agility and speed with which ESMA has developed the prosed guidance, and believe the Consultation is an important step towards building a comprehensive EU global framework for digital assets. As such, the response to the Consultation looks to provide suggestions of areas where additional specificity and practical implementation measures may be needed for effective implementation of the guidance.

GDF has worked with our members to provide a constructive assessment of how to overcome challenges in implementing the guidance. Through this process, the Working Group has identified key areas that may require further drafting consideration or additional guidance for purposes of clarity, proportionality, and effective implementation. The core areas identified are:

1. **Proportionality for Reasonable Reporting Encouraged**
2. **Further Consideration of Firm Size and Cost of Implementation**
3. **Guidance Encouraged for Aspects where Additional Monitoring and Reporting Factors may Diverge from TradFi Requirements**

1. Proportionality for Reasonable Reporting Encouraged

GDF members would note that some requirements within the Consultation, such as the STOR template as proposed, may go beyond what firms can reasonably report. The requirement for STORs to include aspects of the functioning of the ledger itself, including aspects such as consensus mechanisms, adds another layer of complexity which certain firms, depending on their technology stack may not have access to.

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.

To require firms to ensure that their monitoring systems can analyse and detect any and all suspicious activities related to DLT operations, is in effect to mandate that they have supervision and risk management over the whole of the blockchain. GDF feels that this is

neither proportionate, nor appropriate. Requiring firms to have in place continuous monitoring of all orders and transactions, regardless of whether they occur on or off a trading platform, is neither reasonable nor achievable. This would be equivalent to requiring a traditional retail bank to have risk monitoring systems for all activities taking place on the internet upon which its banking applications run. Instead of this approach, we would encourage ESMA to focus on STOR requirements which highlight how a firm is mitigating risk for their critical business services.

2. Further Consideration of Firm Size and Cost of Implementation

GDF would note that for many firms, especially smaller ones, the requirements proposed throughout the Consultation could be resource-intensive and complex. We would reiterate that the requirements should be proportionate to both firm size, as well as the scope of their activities.

Reporting requirements should be implemented where a firm can reasonably report on the activities they are conducting and have sight of within the market. A regulatory grace period would also be beneficial for smaller players and would support ESMA's aim of a level playfield as MiCAR is implemented and firms work towards compliance.

3. Guidance Encouraged for Aspects where Additional Monitoring and Reporting Factors may Diverge from TradFi Requirements

For some areas of the proposed guidance, GDF notes that certain forms of market abuse referenced within the guidance may not be appropriate for crypto-assets such as 'Trash & Cash', 'Marking the Open' and 'Marking the Close'. These are specific references to behaviours within TradFi markets that do not have a direct parallel in crypto-asset markets.

Another example is the appropriate factors which are used to determine in what territory or jurisdiction an asset is trading. These factors will be different in crypto-asset markets, as unlike TradFi there are no tickers listed on a particular exchange. A different approach may be required to facilitate the identification of suspicious orders/transactions/behaviours.

Response to the Consultation Paper (CP): Questions for Public Consultation

Please note that given our focus areas set out in the executive summary, we have not responded to each question in the ESMA consultation. Instead, we have provided feedback in input on the specific questions and chapters that are relevant to the key areas. Where we have not provided further feedback, we are supportive of the Technical Standard proposals that have been set out.

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.

GDF members believe that the definition of persons professionally arranging or executing transactions (PPAET[1]) could be challenging to implement as the definition is quite broad. As entities prepare for MiCA implementation, and prepare their monitoring systems to comply, they will also need real-time and deferred analysis of trading activities, including the ability to replay order book data and generate alerts for potential market abuse. We would note that given how broad the current definition is, this may require additional updates to the monitoring

[1] Please note an expanded discussion of PRAET has been included in Annex 1of this response.

systems firms have in place, and thus we would encourage a regulatory grace period as firms prepare.

Furthermore, the current definition would also apply to broker dealers who may not have the capability to detect market abuse as an exchange would, if they are only executing one leg of the transaction. We would encourage the requirements be implemented in a manner that is proportionate to what each firm, and their business model can reasonably report. GDF members believe that this would support compliance across the whole of the ecosystem, and also enable authorities to have a more accurate view of where market abuse is occurring.

Within the broad definition, we would also recommend excluding CASPs whose sole business model is to provide custody and administration of crypto-assets. As the storage and issuance of crypto-assets is not involved in activities that result in market abuse, we would recommend this sit outside of the scope of the requirements.

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.

Finally, GDF would note that for many firms, especially smaller ones, developing and maintaining such sophisticated systems could be resource-intensive and complex. We would reiterate that the requirements should be proportionate to both firm size, as well as the scope of their activities. Reporting requirements should be implemented where a firm can reasonably report on the activities they are conducting and have sight of within the market. Additionally, as noted, a regulatory grace period would also be beneficial for smaller players and would support ESMA's aim of a level playfield as MiCAR is implemented and firms work towards compliance.

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.

GDF notes that one aspect which may require additional solutions from industry, as well as cross-border collaboration, is the appropriate factors which could be used to determine in what territory or jurisdiction an asset is trading. These factors would be different in crypto-asset markets than in a TradFi context where you have tickers listed on a particular exchange. This is not the case for most digital exchanges so a different approach may be required to facilitate the identification of suspicious orders/transactions/behaviours.

Additionally, as noted under Q1, we would encourage ESMA to consider if the prescribed requirements are feasible, especially for smaller firms. This assessment should also consider the costs of implementation and what is proportionate and appropriate depending on the size and business model of the firm in question.

Overall, GDF supports the implementation of appropriate market surveillance tools in the crypto asset ecosystem in order to foster markets that are safe and transparent. 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.

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

GDF members would note that in some cases the STOR proposed template may go beyond what firms can reasonably report. The requirement for STORs to include aspects of the functioning of the ledger itself, including aspects such as consensus mechanisms, adds another layer of complexity which certain firms, depending on their technology stack may not have access to.

To require firms to ensure that their monitoring systems can analyse and detect suspicious activities related to DLT operations, is in effect to mandate that they have supervision and risk management over the whole of the blockchain. GDF members do not believe that this is either proportionate, or appropriate. Requiring firms to have in place continuous monitoring of all orders and transactions, regardless of whether they occur on or off a trading platform, is neither reasonable nor achievable. This would be equivalent to requiring a traditional retail bank to have risk monitoring systems for all activities taking place on the internet upon which its banking applications run. Instead of this approach, we would encourage ESMA to focus on STOR requirements which highlight how a firm is mitigating risk for their critical business services. Similar to requirements within traditional financial services, it is crucial for firms to have appropriate business continuity planning and risk mitigants in place, and GDF is supportive of the principle of the STOR template, subject to the following revisions which would either not provide relevant information or would not be achievable for most firms to implement:

- Location (where the behaviour on the DLT occurs) – as the blockchain is located in the ether this would be difficult to pinpoint. The IP address of miners/validator nodes could be located but would not provide the authorities with the information needed to detect and prevent market abuse.
- Date of Birth
- Digital Token Identifier (DTI)
- Legal Entity Identifier (LEI) of the CASP
- Full address information of underlying client (person or entity)
- Information about the employment of the underlying client (person or entity)
- Account number

The exclusions noted above, are raised because the STOR template as currently set out includes 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. Expanding on the above, GDF would support an approach where 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" is 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 purpose and may create additional burden for reporting suspicious behaviour in the context of market abuse. Finally, the concept of the 'location' is

largely irrelevant for distributed ledger technologies due to the decentralised nature of the network and the use of IP masking techniques like VPNs.

GDF supports a holistic approach to prevention of financial crime and market abuse, yet the above requirements go above and beyond what would be relevant for detection and prevention. We would encourage the authorities to take a more balance and proportionate approach, working with industry to achieve the necessary aims and foster compliance across the ecosystem.

Finally, GDF members also feel that further clarification on what is meant with "aspects connected with the functioning of the DLT" would be beneficial as mentioned in paragraph 27 of the Consultation.

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?

GDF members would note that certain forms of market abuse referenced within the guidance may not be appropriate for crypto-assets such as 'Marking the Open' and 'Marking the Close'. These are specific references to behaviours within TradFi markets that do not have a direct parallel in crypto-asset markets. While some crypto surveillance systems providers do use language like, "Trash and Cash" and "Pump and Dump", overall, GDF would not advocate for a one for one transfer of Market abuse typologies from MIFID II/MAR. We would request instead that ESMA continue to consult with the industry as abuse scenarios are discovered and evolve. Furthermore, we would note that 'Insider Dealing' as currently defined would not be covered solely by external market abuse tools and should also be covered and monitored for by teams such as internal audit.

More broadly, to effectively monitor and report suspicious activities involving crypto-assets, establishing clear and standardized parameters and naming conventions is essential. Regulatory bodies and industry stakeholders should work together to define and implement these standards, ensuring all parties involved are consistently updated and trained on their application. Standardized practices would enhance transparency, traceability, and the efficiency of detecting market abuse, leading to better data analysis, easier pattern recognition, and more effective regulatory oversight.

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?

No, as noted above under Q3 'location' is not an applicable requirement as the blockchain is located in the ether this would be difficult to pinpoint. The IP address of miners/validator nodes could be located but would not provide the authorities with the information needed to detect and prevent market abuse.

Moreover, the information could be impossible to acquire, as Centralized Crypto Exchanges (CEXs) would not have access to information on where validators and other actors are located within a permissionless distributed context. Therefore, focusing on geographic locations wouldn't be effective for ongoing supervisory purposes surrounding market abuse. The burden of tracking such information may have the unintended consequence of less information sharing

by CASPs, inhibiting regulators from the appropriate signals needed to start a deeper investigation.

Q6: Is there any other element or information relevant to crypto-asset markets that in your view should be included in the template? Please explain.

We would note that the sharing of some of the information requested may contradict GDPR and may not be able to legally be shared, especially as some information may need to be shared on a cross border basis. For the requirements identified above GDF would encourage a more proportionate approach.

Q7: 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.

As noted above, GDF supports a holistic approach to prevention of financial crime and market abuse, yet the above requirements go above and beyond what would be relevant for detection and prevention. Given this, we would encourage the authorities to take a more balance and proportionate approach, working with industry to achieve the necessary aims and foster compliance across the ecosystem.

GDF members further note that for many smaller firms in particular these systems will likely be costly to implement and maintain. There will also be a cost to training and hiring the appropriate talent, risk managers and compliance staff. As noted under Q1 we would encourage a regulatory grace period as firms prepare to implement the requirements.

Overall GDF appreciates that investments will be needed in surveillance systems, data analytics, and blockchain monitoring as well as the benefits that can arise from advancement of technology and the introduction of modern, cost-efficient risk monitoring and infrastructure. This is a crucial part of the ecosystem, but we would note that the systems implemented should be proportionate and reasonable, in line with a firm's business model and their role in the ecosystem.

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?

GDF members have raised concerns on the proposal set out under paragraph 74, indicating that firms should consider the environmental, social and governance (ESG) preferences of clients. Given that this could vary widely both by EU NCA implementation, as well as by definition and interpretation of preference and appropriateness, it could significantly impact firms' ability to offer products consistently across the EU. This could have the unintended consequence of being both harmful to competition and may also increase fragmentation in MiCA implementation.

Furthermore, given that the implementation of ESG requirements more broadly in the EU has been highly politicised, and that some of these frameworks are still evolving, such a requirement could have a disproportionate impact on crypto and digital asset markets. It may also result in high compliance costs and an outsized burden on firms as they may need to significantly adjust their offering across different EU member states.

Expanding on the above, GDF acknowledges and welcomes that ESMA has recently published final guidelines on certain aspects of the MiFID II suitability requirements and that these guidelines aim to ensure a consistent and harmonized application of suitability requirements, including sustainability considerations. Yet despite MiFID II coming into force in January 2018, GDF would note that most ESG aspects are still being developed and evolved and across EU member states, and within this there are varying levels of compliance and harmonisation. Therefore, GDF members believe that to impose a consistent approach regarding suitability regimes between MICAR and MIFID II would be premature, have the unintended consequence of being operationally punitive, and could potentially cause fragmentation. This may also result in EU crypto-asset markets being less competitive given the global nature of the crypto-asset markets more broadly.

Finally, we would also note that paragraphs 64 and 92 seem to be at odds. In paragraph 64 the Consultation notes that "For instance, under MiFID II, the extent of the obligations of an investment firm under the suitability requirements may vary depending on the level of complexity and riskiness of the financial instruments considered as part of the advice or portfolio management services. Under MiCA, **such differentiation is less relevant as there is no such thing as a 'safe' crypto-asset."** Yet in paragraph 92 the consultation states that, "ESMA is of the view that the suitability assessment (matching clients with suitable crypto-assets) entails a thorough assessment of the availability of alternative investments, **taking into account products' costs and complexity.**" GDF would welcome clarification from ESMA on complexity assessments of products, and the requirements for firms to assess suitability in light of these statements. We would note that if the MiFID II requirements are to be implemented fully, this will be a significant compliance requirement for firms, in particular those which are smaller – as noted under several previous questions.

Q9: 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.

Yes, as noted above under Q3 GDF would note that there are several areas where the requirements do not fit appropriately with crypto-assets and crypto-assets markets. We would encourage other tools and requirements be implemented which may more accurately detect and prevent market abuse within the ecosystem.

Since the crypto markets are evolving rapidly, GDF believes that all ESMA guidelines, not exclusively regarding suitability regimes, should remain clear and consistent for crypto-assets. It is also crucial for guidelines to be adaptable and forward looking to avoid imposing inaccurate risk assessments and having outsized impacts on the industry which may negatively impact the EU's competitiveness in digital markets. Guidelines will need to be future proof in order to adapt to changing risk landscapes, while also fostering innovation. GDF welcomes the opportunity to continue to collaborate with ESMA in the hope that our insights can inform effective guidelines.

Q10: Do you agree with the approach followed by ESMA regarding periodic statements provided in relation to portfolio management of crypto-assets?

Yes, GDF is supportive of the approach.

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.

Yes, GDF is supportive of the approach, however we would also bring ESMA's attention to one specific point in relation to the scope of transfer services.

In MiCA, transfer services are defined as "*providing services of transfer, on behalf of a natural or legal person, of crypto-assets **from one distributed ledger address or account to another***". We understand from the extract in bold that the definition of transfer services intends to cover two different types of on-chain transfers, depending on the DLT used:

- The reference to distributed ledger "address" is intended to capture blockchain address relying on **UTXO-based blockchains**;
- The reference to a distributed ledger "account" is intended to capture blockchain addresses relying on **account-based blockchains**.

GDF members note that the intent seems to be from the definition of transfer services contained in MiCA that transfer services are intended to cover **on-chain transfers** facilitated by a CASP (i.e., where crypto-assets move from one blockchain address to another.)

GDF members feel that this contrasts with Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets ("**TFR**") in which transfer services are defined in a different manner:

*'transfer of crypto-assets' means any transaction with the aim of moving crypto-assets from one distributed ledger address, **crypto-asset account** or other device allowing the storage of crypto-assets to another, carried out by at least one crypto-asset service provider acting on behalf of either an originator or a beneficiary, irrespective of whether the originator and the beneficiary are the same person and irrespective of whether the crypto-asset service provider of the originator and that of the beneficiary are one and the same;*

The transfer definition in TFR contains a reference to "crypto-asset account", which is further defined in TFR as:

*'crypto-asset account' means **an account held by a crypto-asset service provider** in the name of one or more natural or legal persons and that can be used for the execution of transfers of crypto-assets;*

GDF members believe that the above definition seems to reference to off-chain accounts managed by CASPs and which allow users to interact with digital asset products. TFR therefore would then apply to off-chain transfers executed between crypto-asset accounts.

By contrast, the definition of transfer services under MiCA seems to indicate that transfer services shall not apply to pure off-chain transfers within the internal systems of a CASP. GDF would welcome ESMA clarifying the draft RTS on this point as there seems to be a reference to crypto-asset accounts in the text of the draft RTS. In particular, point 19 of the draft RTS indicates that:

Crypto-asset service providers should establish, implement, and maintain adequate policies and procedures (including appropriate tools) to ensure that, after execution of individual transfers for crypto-assets, the crypto-asset service provider provides the client with at least the following information:
● *the names of the originator and the beneficiary*

- *the originator's distributed ledger address or* ***crypto-asset account number;***
- *the beneficiary's distributed ledger address or* ***crypto-asset account number;***

This reference to crypto-asset account number here seems to be imported from TFR but in contrast would not align to the context of transfer services under MiCA. GDF would suggest instead that these two bullet points could read "***the originator's distributed ledger address or account***". This would clarify the discrepancy and support broader alignment.

GDF would welcome further clarification from ESMA on this point, and in particular if the RTS intends to cover both on and off chain data, or on-chain transfers exclusively.

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.
As indicated under Q11 above, GDF members would welcome clarity on if the guidelines cover on and off chain transfers, or exclusively on-chain transfers.

Q13: 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?
With respect to the coordination procedures between national competent authorities for detection and sanctioning of cross-border market abuse situations, GDF agrees with ESMA that establishment of detailed procedures for NCAs to exchange information, coordinate investigations, and report on enforcement activities is essential. We would agree that 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 and enhancing regulatory oversight and prioritize cross-border cooperation to address market abuse effectively. GDF is supportive of these aims.

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).

Q15: 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.

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.

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)?

Annex 1: Expanded Discussion of Persons Professionally Arranging or Executing Transactions (PRAETs)

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&As (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".

To assess if validators, miners, or other players in the network could qualify as PPAET, it is important to highlight that each decentralized blockchain networks' native process for processing, ordering, and finalizing user transactions and intents can widely differ. Each network, whether abiding by a Proof-of-Work (PoW), Proof-of-Stake (PoS), or other consensus algorithm, may have unique characteristics in accomplishing the above-mentioned process of settling user transactions and intents onchain. 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 on 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 behavior 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 finalized 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 onchain 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.