17 December 2024
ESMA75-453128700-1278

Final Report

Draft technical Standards specifying certain requirements in relation to the detection and prevention of market abuse under the Markets in Crypto Assets Regulation (MiCA)

Table of Contents

1 Executive Summary

Reasons for publication

The Regulation on Markets in Crypto-Assets (MiCA)[1] requires ESMA to prepare regulatory technical standards (RTS), implementing technical standards (ITS) and Guidelines on a range of mandates for submission to the European Commission. This includes the mandate to develop a draft RTS to specify arrangements, systems and procedures for detecting and reporting suspected market abuse in crypto-assets, the template to be used to report suspected market abuse as well as coordination procedures between the relevant competent authorities for the detection and sanctioning of cross-border market abuse situations.

On 25 March 2024, ESMA published a third Consultation Paper requesting input from stakeholders on ESMA's proposals for the draft RTS on detection and reporting of market abuse and three draft Guidelines. In the consultation, which closed on 25 June 2024, ESMA received 29 responses. The non-confidential responses are available on ESMA's website. This Final Report explains how ESMA incorporated stakeholder feedback received in the public consultation.

In parallel, ESMA sought the advice of the Securities and Markets Stakeholder Group (SMSG) established under Regulation (EU) No 1095/2010. The advice submitted by the SMSG in relation to this consultation is included in Annex III.

Contents

Section 2 provides an introduction to the Final Report and presents the legal basis as well as the mandate for ESMA to develop the RTS. Section 3 recalls the approach proposed in the CP and presents the feedback received from the consultation as well as the proposed way forward in relation to the arrangements, systems and procedures for preventing and detecting market abuse. In particular, with respect to the personal scope of PPAETs for the purpose of Article 92 of MiCA, the Final Report concludes that this should not be defined in the RTS. ESMA will continue gathering evidence and liaise with the European Commission to ensure that appropriate guidance is provided on this matter.

Section 4 recalls the approach proposed in the CP and presents the feedback received from the consultation as well as the proposed way forward in relation to the notification template for reporting suspected market abuse. Notably, the template provides for the identification of the reporting entity, the nature and description of the suspected behaviour, the identification of the suspected person as well as any additional information or documentation.

e Section 5 focusses on the procedures between the relevant competent authorities for the detection and sanctioning of market abuse in case of cross-border situations. This includes provisions on the exchange of STORs between the relevant competent authorities for

detecting cross-border market abuse well as provisions for the purpose of sanctioning those forms of market abuse.

Lastly, this Final Report also includes four annexes. Annex I contains the cost/benefit analysis undertaken in relation to the draft technical standards. Annex II contains the detailed feedback received from respondents. Annex III includes the advice received by ESMA from the Securities and Markets Stakeholder Group (SMSG) while Annex IV contains the draft technical standard.

Next Steps

The draft RTS is submitted to the European Commission for adoption. In accordance with Articles 10 of Regulation (EU) 1095/2010, the European Commission shall decide whether to adopt the technical standard within 3 months.

[1] Regulation (EU) 2023/1114 of the European Parliament and the Council of 31 May 2023 on markets in crypto-assets (OJ L 150,9.6.2023, p. 40–205).

2 Introduction

Article 92(2) of MiCA:

"ESMA shall develop draft regulatory technical standards to further specify:

(a) appropriate arrangements, systems and procedures for persons to comply with paragraph 1;

(b) the template to be used by persons to comply with paragraph 1;

(c) for cross-border market abuse situations, coordination procedures between the relevant competent authorities for the detection and sanctioning of market abuse."

1. Title VI of MiCA establishes rules to deter market abuse with respect to trading of crypto-assets. As part of these rules, MiCA prohibits insider dealing, unlawful disclosure of inside information and market manipulation, and includes specific obligations for the prevention and detection of abusive behaviours.

2. More precisely, Article 92(1) of MiCA requires that persons professionally arranging or executing transactions (PPAETs) in crypto-assets should have in place effective arrangements, systems and procedures to prevent and detect market abuse. In addition, MiCA requires PPAETs to report to the competent authority of the Member State where they are registered or have their head office (or in the case of a branch, the Member State where the branch is situated) any reasonable suspicion regarding an order or transaction as well as other aspects of the functioning of the distributed ledger technology (DLT), such as the consensus mechanism, where there might be circumstances indicating the existence of market abuse.

3. Article 92(1), second subparagraph, also sets out that competent authorities receiving a suspicious transaction or order report (STOR) should transmit such information immediately to the competent authorities of the trading platforms concerned.

4. In addition, Article 92(2) of MiCA mandates ESMA to draft an RTS to further specify: (a) appropriate arrangements, systems and procedures for persons to comply with Article 92(1); (b) the template to be used by persons to comply with Article 92(1); (c) for cross-border market abuse situations, coordination procedures between the relevant competent authorities for the detection and sanctioning of market abuse.

5. Against this background, on 25 March 2024, ESMA published a Consultation Paper (CP)[2] presenting a draft RTS specifying those requirements related to the detection, prevention and reporting of suspected market abuse.

[2] https://www.esma.europa.eu/sites/default/files/2024-03/ESMA75-453128700-1002_MiCA_Consultation_Paper_-_RTS_market_abuse_and_GLs_on_investor_protection_and_operational_resilience.pdf

6. The CP also covered mandates related to investor protection and operational resilience. However, as far as the questions related to the draft RTS on market abuse are concerned, ESMA received feedback from a number of stakeholders ranging from 16 to 29, depending on the question.

7. It is also worth noting that, in accordance with Article 37 of Regulation (EU) No 1095/2010, ESMA requested the opinion of the Securities and Markets Stakeholder Group (SMSG) who provided its advice on 21 June 2024[3].

3 Appropriate arrangements, systems and procedures for preventing and detecting market abuse

3.1 Proposal in the CP

8. In order to effectively design the appropriate arrangements, systems, and procedures for complying with the regime, ESMA analysed in the CP the personal scope of the obligation to submit STORs as well as the type of orders, transactions and behaviours that should be reported by means of a STOR.

9. ESMA's proposals are summarised in the following paragraphs.

Personal scope of the Article 92 regime

10. With respect to the personal scope of the MiCA STOR regime, ESMA concluded that the following persons should be considered as PPAETs for the purpose of Article 92 of MiCA:

- CASPs operating a trading platform[4];
- CASPs providing services related to crypto-assets such as reception or transmission of orders for crypto-assets on behalf of clients, execution of orders for crypto-assets on behalf of clients, portfolio management of crypto-assets, exchange of crypto assets for funds, exchange of crypto-assets for other crypto assets[5];
- Persons dealing on own account in crypto-assets on a professional basis or as part of their business activity. The fact that they have staff or a structure dedicated to systematically deal on own account, such as a trading desk are indicators to consider a person as a PPAET.

Material scope of the prevention and detection mechanism

[3] https://www.esma.europa.eu/sites/default/files/2024-06/ESMA24-229244789-5075_SMSG_Advice_on_MiCA_package__3.pdf
[4] See recital (21) of MiCA.
[5] See recital (21) of MiCA.

11. In relation to the material scope of the prevention and detection mechanism, ESMA noted in the CP that Article 92 of MiCA differs from Article 16 of MAR as the former extends the obligation to report as a STOR "(..) **other aspects of the functioning of the distributed ledger technology such as the consensus mechanism**" beyond "order or transaction, including any cancellation or modification thereof".

12. ESMA also highlighted in the CP that only orders, transactions, and other aspects of the distributed ledger technology that suggest the existence of market abuse should be reported by means of a STOR. STORs should not cover other types of fraud without an identifiable connection with market abuse[6] such as scams, payment fraud or account takeover.

Arrangements, systems and procedures

13. ESMA noted in the CP that the framework designed under MiCA as well as the empowerment for ESMA to develop a draft RTS pursuant to Article 92(2) of MiCA, resembles, respectively, the obligation and the mandate under Article 16 of Regulation (EU) No 596/2014[7] (MAR) on STORs for financial instruments.

14. Against this background, ESMA considered Article 16 of MAR and Commission Delegated Regulation (EU) 2016/957[8] (hereinafter CDR 2016/957) as a starting point for the mandate on the arrangements, systems, and procedures for PPAETs to prevent and detect market abuse.

15. In light of that, ESMA proposed replicating some of the requirements imposed to PPAETs and trading venues under CDR 2016/957 in the draft RTS because most of the abusive behaviours occurring in crypto-asset markets follow patterns and schemes already observed in the traditional finance's space. Additionally, ESMA included requirements related to the specific nature of transactions in crypto-assets, such as the effective and ongoing monitoring of the functioning of the distributed ledger technology.

16. More in detail, ESMA's draft RTS required PPAETs to establish arrangements, systems and procedures that ensure an effective and ongoing monitoring of transactions, orders, and other aspects of the functioning of the distributed ledger technology and allow for the reporting of STORs to the relevant NCA. At the same time, considering that the size, nature, and scale of the business activity carried out by PPAETs may vary significantly, ESMA considered that systems, arrangements, and procedures

[6] As highlighted in the CP, ESMA staff consider this point important because the IOSCO consultation paper on Policy Recommendations for crypto and digital asset markets extend the market surveillance requirements applying to CASPs beyond market abuse strictly speaking. Examples of these requirements are that CASPs should be required to have "requirements, in line with FATF recommendations for AML-CTF, including (amongst other things) customer due diligence requirements".
[7] Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC.
[8] Commission Delegated Regulation (EU) 2016/957 of 9 March 2016 supplementing Regulation (EU) No 596/2014 of the European Parliament and of the Council with regard to regulatory technical standards for the appropriate arrangements, systems and procedures as well as notification templates to be used for preventing, detecting and reporting abusive practices or suspicious orders or transactions

developed by PPAETs should be proportionate and appropriate to comply with the STOR regime.

17. ESMA also proposed that these systems, arrangements, and procedures should be updated regularly to ensure that they remain fit for purpose and therefore introduced a requirement for PPAETs to assess them regularly, at least on an annual basis, and update them when necessary. In addition, the draft RTS also suggested that PPAETs should document in writing those systems, arrangements and procedures and keep track of any changes or updates.

18. In the draft RTS, ESMA also proposed that those systems should have certain technical capabilities, including software capable of deferred automated reading, replaying and analysis of order book data. Such software should also have sufficient capacity to prevent market abuse in real-time and operate in an algorithmic trading environment.

19. Furthermore, ESMA deemed that such systems, arrangements, and procedures should cover the full range of trading activities undertaken by PPAETs and should allow PPAETs, to analyse every transaction executed and order placed, modified, cancelled, or rejected in the systems, both on and outside of a trading venue. Similarly, the draft RTS presented in the CP established that CASPs operating a trading platform should also develop systems that allow for the analysis of every order entered or transaction concluded on their platforms.

20. To ensure that PPAETs are able to analyse behaviours that might constitute market abuse in a timely manner, the draft RTS required their systems and arrangements to produce automated alerts to be followed by an appropriate level of human analysis. Considering the importance of the staff involved in the prevention and detection of market abuse, the draft RTS determined that they should also receive dedicated trainings on a regular basis.

21. The draft RTS foresaw that PPAETs may delegate their prevention and detection activity, including the performance of data analysis and generation of alerts, to a third party or to a person of the same group. However, to ensure that PPAETs remain in control of those functions, the draft RTS imposed some requirements: the existence of a written agreement between the parties, the continuous access of the PPAET to the relevant information and the obligation of the PPAET to retain the expertise to assess the work conducted by the service provider.

22. A PPAET might analyse orders, transactions, and other aspects of the functioning of the DLT but conclude that a STOR should not be submitted. In such a case, the PPAET should record the rationale for its conclusions. To ensure that PPAETs have the necessary information to elaborate on the analysis carried out, the draft RTS required them to maintain information on the suspicious behaviour for a period of five years and to provide it to the relevant NCA upon request.

23. Lastly, to enable NCAs to investigate STORs in a timely fashion, ESMA also proposed in the CP that STORs should be submitted without delay, as soon as a reasonable

suspicion is formed, noting that additional information might be submitted at a later stage if needed. The means for transmitting such a STOR are the electronic ones specified by the relevant NCA.

3.2 Feedback from the consultation

Personal scope of the Article 92 regime

24. ESMA sought the views from market participants on the types of entities in the crypto-asset space that should be considered as PPAETs. In particular, ESMA asked whether miners/validators and CASPs providing custody and administration of crypto-assets on behalf of clients should be considered as PPAETs for the purpose of Article 92 MiCA.

25. The feedback received was almost unanimous in excluding miners and validators from the personal scope of Article 92 of MiCA. It is possible to identify two main arguments supporting this position.

26. First, in the blockchain networks where miners and validators do arrange the order of the transactions, they do it to maximise their profits according to the Maximum Extractable Value (MEV). As opposed to traditional finance, where the transactions are strictly arranged according to the time of execution, miners and validators select a group of transactions (i.e., a 'block') that are not organised according to the time of execution. They are structurally incentivised to arrange and prioritise transactions according to their value and to the fees that the parties are willing to pay to prioritise them. Proponents of MEV argue that these incentives provide a large number of benefits to the market[9].

27. At the same time, these replies also considered that in most cases miners and validators lack the incentives to commit market abuse. Therefore, for these stakeholders MEV cannot be systematically assimilated to market abuse, despite some MEV practices being clearly abusive. The responses also noted that there is ongoing work in the industry and academia to identify those practices that constitute market abuse and implement technical solutions to disincentivise them.

[9] Aiding price discovery, **creating more efficient markets** across centralised and DEX platforms, across chains and tapping into other off-chain liquidity sources such as private counterparties - creating tighter spreads across various networks and enabling users to access the prices and liquidity of off-chain venues while staying on-chain. Enabling **arbitrage** between decentralized exchanges leading to **price convergence**. Enabling **liquidations to happen more quickly to protect lenders. Reducing gas costs**, **transaction latency, conditional transaction execution** and offering the possibility of strengthening security (via distributed participation in the network). Enabling user optionality to **access faster transaction execution** (particularly beneficial for high frequency traders / more price-insensitive users). Options to avoid market slippage are available in wallets and dApps, so users can elect to execute their transactions without "slippage" protection by paying a higher execution price, as an alternative to setting high gas fees. Providing **end users rebates**, in certain instances, where a portion of rewards received by participants such as searchers are passed back to the end user.

28. Second, while miners and validators are structurally prevented from rearranging transactions in Ethereum, other players (searchers and builders) might commit market abuse by rearranging the order of the transactions.

29. Likewise, most of the responses received considered that CASPs providing solely the service of safekeeping and administration of crypto-assets should not be considered as PPAETs. These respondents' main arguments were based on the proportionality principle, since these CASPs do not manage or execute transactions and lack the necessary internal controls or the access to the information necessary to detect abusive behaviour.

30. Finally, a limited number of responses suggested excluding CASPs offering only transfers of crypto-assets from the PPAET category. These responses noted that Article 1 of the RTS on record-keeping by CASPs included within the definition of "executing a transaction" "transfer of crypto assets to or from accounts". For these stakeholders i) the mere transfer does not give rise to market abuse practices; and ii) it is challenging to conceive how a CASP solely providing this service could identify reportable behaviour.

Arrangements, systems and procedures

31. Most of the feedback received was supportive of the proposal, including the advice provided by ESMA's SMSG. Nonetheless, it is possible to identify the following areas of concern for stakeholders, mostly about the specific application of the proportionality principle:

    - The risk of market abuse (e.g. on the interaction between the scale of the PPAETs activity and the size of the crypto-asset market) should be factored in to determine whether the proportionality principle should apply. Accordingly, the proportionality principle should not in any case involve that the PPAET's activity implies risks of market abuse at a material level;

    - The capacity of PPAETs to monitor "other aspects of the functioning of the distributed ledger technology";

    - The obligation to monitor off-chain and on-chain transactions. At the same time other responses supported that PPAETs monitor off-chain and on-chain data. For these respondents most of trading takes place off-chain, making this data critical not only for market abuse purposes but also for anti-money laundering and counter-terrorism financing. One of them noted that the integration of both data sets is complex because the execution and settlement of on-chain transactions may take from a few minutes up to one hour. Other responses considered that PPAETs should not be forced to monitor on-chain activity when operating only in the off-chain environment.

32. Other responses considered that small firms would be heavily impacted by these proposals and suggested instead that:

- Given the implementation costs of in-house surveillance systems, small firms should be able to outsource these systems; and

- They should be provided with flexibility in the periodicity of periodic reviews (that should be 18 months for SMEs whereas large firms should undertake them every 12 months).

33. Finally, the SMSG considered that outsourcing the task of prevention and detection of market abuse might entail systemic risks (e.g. when several PPAETs delegate it to the same provider), asking the relevant authorities to monitor the competition and concentration levels of the market in relation to the outsourced activities.

34. Other market participants' responses proposed setting a "minimum common denominator" applicable to all PPAETs broadly in line with the original proposal, including real-time or near-real time monitoring, in-house or third-party surveillance software (tested, capable of identifying all relevant abusive trading and periodically reviewed), adequate staff, monitoring for employees' insider trading and annual review of the market abuse risk.

35. Additionally, ESMA received a number of suggestions in relation to specific articles of the draft RTS:

    - How trading platforms should apply the requirement of monitoring irrespective of "whether the orders were placed, or transactions executed on or outside a trading platform";

    - Whether the "audits" mentioned in Article 2(3)(b) should be internal or external.

36. One respondent requested a clarification of what should be considered as market abuse "likely to be committed" and about the human analysis reflected in Article 5.

37. Three responses asked for further specification of the timing of submission of STORs in Article 6.

38. Three other respondents considered that the RTS should be technology-neutral and remain applicable to an evolving trading environment, where artificial intelligence and machine learning are increasingly present.

3.3 ESMA's assessment and next steps

Personal scope of the Article 92 regime

39. A significant number of respondents considered that miners and validators should be excluded from the category of PPAETs based on their limited capacity of committing market abuse. Some stakeholders proposed to incorporate searchers and builders into the PPAET category, e.g. due to their capacity to arrange the order of transactions in the Ethereum blockchain.

40. It seems necessary to differentiate between the concept of PPAET and the entities that could commit market abuse. Article 92 of MiCA imposes the obligation to report suspicious orders or transactions on PPAETs, whereas Article 86 of MiCA clarifies that the articles concerning market abuse "*apply to acts carried out by any person concerning crypto-assets that are admitted to trading or in respect of which a request for admission to trading has been made*" (emphasis added).

41. In other words, any person can commit market abuse under MiCA, irrespective of its role in the market. For instance, Article 89(5)(c) of MiCA determines that the prohibition of insider dealing applies to any person "having access to the information through the exercise of an employment, profession or duties or in relation to its role in the distributed ledger technology or similar technology". As a consequence, miners, validators, searchers, builders, depositories, and custodians could be held liable for market abuse if they breach Articles 89, 90 or 91 of MiCA.

42. However, the capacity of certain entities operating in the crypto-space to commit market abuse should not automatically lead to the inclusion of these types of entities into the PPAET category.

43. The identification of the persons who should be considered as PPAETs also depends on the capacity of those persons to monitor a portion of the crypto-assets landscape (including their own activity) and identify potential market abuse cases.

44. In particular, ESMA notes that the responses received did not elaborate on whether a miner, validator, searcher or a builder have visibility about the activity carried out by their peers or other crypto-asset market participants. Therefore, at this stage ESMA cannot determine whether these actors could be in a position to report suspicious activities.

45. There are also other arguments suggesting that these players should remain out of the scope of the prevention and detection obligation under MiCA. Firstly, the role of miners and validators is evolving and, according to these sources, the evolution goes in the direction of a limited presence of MEV's negative externalities. This is achieved by different means, including fair transaction sequencing, first-come-first-served, encrypted mempools or preference matching. Secondly, considering miners and validators within the category of PPAETs could incentivise them to leave or avoid establishing in the EU, which may complicate supervision of EU CASPs who may outsource services to these entities and push innovation offshore.

46. On that basis, ESMA's view is that miners, validators, searchers, and builders should not be considered as PPAETs for the purposes of the prevention and detection of market abuse.

47. Likewise, the responses received consistently indicate that CASPs solely offering the services of custody and administration of crypto-assets should not be included in the PPAET category, since they may not have the access to the information necessary to detect abusive behaviour as they do not execute transactions. ESMA reiterates that

the identification of certain market players as PPAETs not only depends on the market abuse risk they and their clients pose to the market but also on their capacity to monitor a portion of the crypto-assets landscape and identify potential market abuse cases.

48. ESMA also takes stock of the feedback received about CASPs providing solely the transfer of crypto assets to or from accounts regarding their limited visibility on the activity of their clients.

49. Despite having carried out such an analysis, ESMA came to conclude that the personal scope of PPAETs should not be defined in the RTS. From a practical perspective, any positive definition of PPAETs in a level 2 instrument would be relatively rigid and would render possible necessary adjustments coming from the building up of supervisory experience complex to perform.

50. At the same time, ESMA also acknowledges that specifying the scope of PPAETs, and as a consequence the scope of application of the requirements in the RTS, is critical for the successful implementation of MiCA in relation to the prevention and detection of market abuse. As a result, ESMA will continue gathering evidence and liaise with the European Commission to ensure that appropriate guidance regarding the personal scope of Article 92 of MiCA is offered once the technical standard is adopted.

Arrangements, systems and procedures

51. ESMA notes the support received from most of the responses to the consultation.

52. At the same time, ESMA also found contradicting messages from the responses to the consultation: some market participants request setting out a “minimum common denominator” that should be applicable to all reporting entities while other stakeholders request further specification of certain requirements to ensure that the principle of proportionality is applied, in particular with respect to smaller players.

53. In this sense, the draft RTS included a set of requirements for PPAETs which broadly coincides with what is proposed as a minimum common denominator by some respondents. At the same time, this set of requirements covers a wide range of activities, making extremely complex to specify these requirements for each specific sub-type of market participant.

54. It is the task of each PPAET to assess the scale, size, and nature of its own business activity, including the risk that its activities, or the activity of its clients pose to the market (recital (2) of the RTS) and determine its own arrangements, systems and procedures accordingly. ESMA also notes that the approach followed in the proposed RTS is the same successfully followed in Commission Delegated Regulation 2016/957 supplementing MAR. This is without prejudice of further clarifications that ESMA or NCAs may provide in the future. At the same time, and consistently with recital (95) of MiCA, the proportionality principle impacts different parts of the RTS.

55. The SMSG advised that the risk of market abuse does not only depend on the scale, size and nature of the PPAET's business activity but it also depends on the interaction between the scale of the PPAET's activity and the size of the crypto-asset market. In this context, the SMSG suggested that the application of the proportionality principle should never involve that the PPAET's activity implies risks of market abuse at a material level. ESMA understands that the SMSG refers to PPAETs having a significant or dominant position in a specific area of crypto-assets markets.

56. The draft RTS already established in Article 2(3) that the arrangements, systems, and procedures that PPAETs must have in place should be appropriate and proportionate in relation to the "scale" of their business activity. Likewise, recital (2) of the draft RTS indicated that, "The analysis of the appropriateness of the systems should include the risk that the activities of the person professionally arranging or executing transactions or its clients poses to the market".

57. ESMA agrees that having a significant or a dominant position in a segment of the crypto-asset markets should be included in the assessment of the "scale" of the PPAET activity, leading to higher demands in terms of arrangements, systems, and procedures to be adopted. Therefore, the RTS have been amended to reflect this point.

58. However, it would not be consistent with the importance of the detection and prevention of market abuse to fine-tune the periodicity of the review of these arrangements, systems and procedures according to the size of the PPAET. Therefore, ESMA has kept the periodicity of these reviews at 12 months.

59. Likewise, one market participant questioned whether the "audits" mentioned in Article 2(3)(b) should be internal or external. This respondent noted that external "audits" are not prescribed by MiCA. Moreover, this respondent considered that, PPAETs should not need periodic external audits on the basis of the proportionality principle.

60. ESMA agrees that PPAETs may decide to undertake an external or an internal audit of their arrangements, systems, and procedures to prevent and detect market abuse in accordance with the scale, size and nature of their business activity. The reference to 'internal review' in the same provision of Article 2(3)(b) should be understood as a complementary exercise to the audit, conducted by the function within the PPAET responsible for the arrangements, systems and procedures to prevent and detect market abuse.

61. ESMA recognises that smaller market participants might have limited resources to set-up in-house arrangements, systems, and procedures to prevent and detect market abuse. In line with that, the draft RTS allows for the outsourcing of these tasks in case the economic burden of setting up their own in-house arrangements is excessive but also for other specific business reasons.

62. At the same time, while ESMA agrees that the relevant authorities may need to monitor the competition and concentration levels of the market related to the outsourced

activities, it also notes that this competence might not fall within the remit of NCAs and may correspond to the national or EU competition authorities.

63. As regards the concerns expressed regarding the capacity of PPAETs to monitor "other aspects of the functioning of the distributed ledger technology", ESMA notes that this is a requirement set out in MiCA. At the same time, the draft RTS clearly indicates that the arrangements, systems and procedures should cover *the full range of trading activities undertaken by the persons professionally arranging or executing transactions in crypto-assets*. As a consequence, the regulatory expectation is not an ongoing monitoring of the functioning of the consensus mechanism as a whole but only in relation to those transactions that reach the PPAET.

64. The same principle should apply to the monitoring activity of CASPs operating a trading platform: PPAETs are only expected to monitor what falls under their business activity. As a consequence, CASPs operating a trading platform should not monitor orders placed or transactions executed outside their trading platform. Likewise, other PPAETs are not expected to monitor the entire market but each and every transaction executed, and order placed, modified, cancelled or rejected inside and outside a trading platform in which they are directly involved.

65. Another topic that raised the attention of respondents to the consultation was the obligation to monitor off-chain and on-chain transactions. ESMA agrees that the monitoring activity of PPAETs should encompass off-chain transactions, where most trading takes place. ESMA is also of the view that this should encompass other data sources, such as on-chain data, as long as this concerns the activity of the PPAET, considering the importance for market abuse purposes.

66. In particular, as regards on-chain transactions, despite the transparent and decentralised nature of most blockchain networks, ESMA considers that PPAETs should monitor on-chain activity falling under their business activity but not what is beyond that. In that sense, on-chain activity should be monitored whenever the PPAET is directly involved in the on-chain transaction (sender, recipient or similar) or the transaction itself involves directly DLT-transactions (e.g. DEX settlement via DLT and cases that can be assimilated to this).

67. Apart from that, ESMA received a number of specific suggestions and questions in relation to specific articles of the draft RTS:

- One respondent requested a clarification of what should be considered as market abuse "likely to be committed" and about the human analysis reflected in Article 5. The reference to cases of market abuse that are "likely to be committed" refers to the identification of circumstances preparing the grounds for market abuse.

- As regards the human analysis, it should always be present in the detection of orders and transactions that could be abusive. The purpose of this provision is to avoid the submission of not sufficiently substantiated alerts as STORs that would "flood" NCAs and ultimately hamper the prosecution of market abuse.

- In relation to the further specification of the timing of submission of STORs, ESMA remains of that view that it should be submitted to the relevant competent authority without delay once a reasonable suspicion was formed.

- Sometimes a suspicious transaction or order may only be detected sometime after it has actually occurred. As indicated in the recitals of the draft RTS, there will always be a tension between the immediate submission of a STOR and its assessment on a case-by-case basis to determine if several orders, transactions or other aspects of the functioning of the distributed ledger technology could be reported in a single STOR. However, this does not mean that reporting persons have an unlimited period of time to reach the point of reasonable suspicion. Where preliminary analysis is required, this should be conducted as quickly as practicable. In such cases, ESMA would expect the reporting person to be able to justify, if requested, the delay according to the specific circumstances of the case.

- Entities should not only notify transactions and orders which they consider suspicious at the time of the transaction, but also transactions and orders which become retrospectively suspicious in the light of subsequent events or information (such as new orders and/or transactions by the same person).

- As regards the reference to “algorithmic trading” in the RTS, ESMA agrees that the RTS should be technology-neutral and remain applicable to an evolving trading environment, where artificial intelligence and machine learning are increasingly present. However, ESMA also considers that the definition of “algorithmic trading” in Article 4(1)(39) of Directive 2014/65 in Markets in Financial Instruments[10] does not diverge in substance from trading strategies benefitting from artificial intelligence or machine learning, since the determination of the specific parameters of the trading strategy is made without human intervention. Accordingly, a definition of “algorithmic trading”, fully in line with the MiFID II definition, has been added to the RTS.

  In line with that, ESMA has not amended the requirement set out in Article 3 of the RTS since the systems used to detect market abuse should have the capacity to operate in an environment where artificial intelligence or machine learning is used. ESMA will continue monitoring the deployment of artificial intelligence and machine learning in financial and crypto-asset markets.

[10] trading in financial instruments where a computer algorithm automatically determines individual parameters of orders such as whether to initiate the order, the timing, price or quantity of the order or how to manage the order after its submission, with limited or no human intervention, and does not include any system that is only used for the purpose of routing orders to one or more trading venues or for the processing of orders involving no determination of any trading parameters or for the confirmation of orders or the post-trade processing of executed transactions.

4 Notification template for reporting suspected market abuse

4.1 Proposal in the CP

68. In the CP, ESMA noted that the notification template for reporting suspected market abuse developed under MAR could be used as starting point given the similarities between the obligations and the mandates under Article 92 of MiCA and Article 16 of MAR.

69. From that basis, ESMA proposed in the CP that the template should include a number of fields allowing for the identification of the person submitting the STOR as well as the transaction or order concerned, the description of the suspicion and, where possible, the identity of the suspected person. In addition, in line with the MAR precedent, the template proposed by ESMA in the CP also provided for additional information and supporting documentation that might be useful in the context of the report.

70. Moreover, ESMA adapted the MAR template to reflect specificities of the crypto-asset markets such as the identification of the crypto-asset (including the type of crypto-asset and/or the trading pair) or of the type of DLT technology used when the reported behaviour relates to aspects connected with the functioning of the DLT.

4.2 Feedback from the consultation

71. Respondents generally welcomed the template presented in Annex II of the CP and agreed with the approach proposed by ESMA. However, some stakeholders considered that that template includes more information than necessary to make a determination on market abuse, and recommended ESMA to streamline the STOR template to ensure that CASPs are able to report information quickly enough to allow NCAs to act upon the STOR without delay.

72. Some of these players also suggested that ESMA should distinguish between what information may be critical and thus required to be provided with each initial submission and what additional information could be provided at a later stage as to favour a more timely and swift submission of STORs. Some of these stakeholders also considered that it would be costly to implement and put in place systems to provide all the required information.

73. These respondents also provided targeted examples of fields which in their view may be removed from the template, such as the description of the DLT, considered unnecessary by some respondents in the context of a STOR submission as this information may not be readily available to the reporting persons or in some other cases it can be already public information. In this respect, there was also a comment inviting ESMA to consider whether the distinction between private/permissioned and public/permissionless DLT should be introduced in the template.

74. At the same time, it is also worth noting that one respondent expressed a different view and suggested being more detailed on the information specific to the DLT on which the transaction or order occurred. In the respondent's view, this could include the blockchain name, the block number and the transaction hash.

75. In addition, respondents provided a number of targeted suggestions to amend some specific fields related to the description of the identity of the person submitting the STOR, the identification of the person responsible for the suspected behaviours, the details of the order to be reported, the nature of the suspicion as well as the additional information and supporting documents.

76. ESMA also received comments in relation to the confidentiality of the information provided in the template as some respondents considered that there should be reassurance that supplying certain information will not constitute a violation of the relevant privacy regulations.

77. Lastly, a few market participants made some general suggestions such as inviting ESMA to develop further guidance to support PPAETs when completing and submitting STORs, providing PPAETs with annual feedback on the quality of the STORs submitted and creating a dedicated portal for the submission of STORs. The more detailed feedback received is presented in Section 6.2 below.

78. In addition, ESMA sought feedback on parameters and naming conventions that would be more adequate to identify suspicious orders, transactions or behaviours related to the functioning of the distributed ledger technology and any references that might be obsolete in relation to crypto-assets. ESMA also invited respondents to provide feedback on any elements that may be missing from the template as presented in the CP.

79. Respondents were of the view that the parameters and naming conventions presented in the CP were generally accurate and did not raise any point that would substantially alter the template. They however made some suggestions, including the addition of a field to identify the wallet address(es) involved in the suspected behaviour as well as the use of a more detailed taxonomy for transactions (e.g. 'swap', 'transfer'), suspicious behaviours (e.g. rug pulls, oracle manipulation, pump-and-dump, etc) and order (e.g. market order, limit order, stop-loss order) types.

80. In relation to other elements relevant to crypto-asset markets that may be included in the template, ESMA received some suggestions including the addition of fields on potential interactions with smart contracts, details of transaction/order volumes and fees associated to it, wallet addresses, transaction hashes or blocks as well as some ancillary information such as market conditions, news or events, social media interactions.

81. On the contrary, a respondent representing a CASP providing different crypto-asset service including the operation of a trading platform reiterated that instead of adding new fields, ESMA should rather streamline the list of parameters in the template.

82. Separately, ESMA also asked whether the concept of 'location' (in the form of an ISO country code) found in Section 2 of the STOR template would be applicable to abusive behaviour detected on a distributed ledger, and whether such information could even be ascertained by the PPAETs reporting a STOR when miners, validator nodes or other entities involved in the preparation of transactions that comprise the DLT network can easily mask their IP addresses through the use of VPNs.

83. Almost all respondents to the question on location of the suspected market abuse occurring on a distributed ledger expressed scepticism about the efficacy or ability of PPAETs to determine location in the context of a permissionless DLT. Some respondents called for the entire location field to be completed by PPAETs on a best effort basis (i.e., 'where available') and cautioned against requiring PPAETs to use sophisticated VPN 'unmasking' techniques to obtain this information.

84. Several respondents specified that location of entities involved in arranging and validating transactions (e.g. a consensus node) should be identifiable in the case of permissioned DLTs because the entities running such nodes are typically subjected to know-your-customer certifications before they can enter the network. In such cases, ESMA would expect the location information to be readily available and therefore reportable in a STOR.

4.3 ESMA's assessment and next steps

85. ESMA took into account the feedback received in the context of the consultation and this section presents ESMA's considerations on the suggestions received as well as the proposed amendments to the template.

86. Firstly, ESMA considered the suggestion to streamline the STOR template to ensure that CASPs are able to report information quickly enough to allow NCAs to act upon the STOR and to distinguish between critical information that should be provided within each initial filing and additional information that could be provided at a later stage.

87. ESMA appreciates the concerns raised by some respondents and agrees on amending some of the fields as presented in the following paragraphs. However, it is worth noting that ESMA would be against fundamentally changing the approach to the template, for instance, by only requiring PPAETs to submit essential information within the STOR and additional information at a later stage (as suggested by some respondents). In that respect, ESMA notes that the MAR precedent has shown that a similar regime works well and that this represents a first step for entities operating in the crypto space to build a strong compliance culture, also with respect to STORs submission. As a consequence, ESMA does not suggest amending the structure of the template.

88. Compared to the version of the template presented in the CP, ESMA has introduced an instructional header requiring PPAETs to fill in all fields in Sections 1-4. However, considering that some of the fields may not be applicable to all STORs or the information may not be available to PPAETs, ESMA provides reporting persons with

the possibility to indicate “NA” and give a brief explanation of the reason why information cannot be supplied. As a consequence, any references to ‘where applicable’, ‘if applicable’ or ‘where known’ etc throughout the template have been deleted as this would be already covered in the option to reply “NA”. While such an approach would not alter the substance of the STOR reporting, it would allow NCAs to receive comprehensive reports and more easily identify the information that PPAETs are not in the position to provide.

89. With the aim of reducing any possible duplication of work on the NCAs’ side, ESMA added a new field asking whether the same facts have already been reported to (other) public authorities to allow NCAs to conduct more efficient follow-ups to the STOR.

90. With respect to the point raised by some respondents on the confidentiality of the information included in the STOR template, ESMA does not see any contrast with the relevant privacy regulations as the submission stems from a sound legal basis as long as the information requested in the template is in the form of a closed list. This is also confirmed by the existence of a MAR precedent where PPAETs are also required to submit similar information to NCAs.

91. Regarding the set of comments received on the description of the distributed ledger technology, ESMA concurs with market participants that the name of the DLT may be sufficient for the purpose of the STOR submission. In that sense, ESMA deems it appropriate to limit the information to the name of the DLT as in some cases additional information on the DLT may be public already or, in contrast, not known to the reporting person. Additionally, ESMA slightly amended the description of the field to make clear that more than one DLT name can be reported whenever the suspicious behaviour involves multiple DLTs. The changes are reflected in the template presented in Annex IV. It is also worth noting that, where relevant, PPAETs may be able to include any additional information under Section 5 of the template.

92. Moreover, in relation to the comment inviting ESMA to distinguish between public (permissionless) and private (permissioned) DLT in the template, while this could be useful in the context of STORs related to the functioning of the DLT, ESMA would limit the information about the DLT to its full name for the reasons explained in the previous paragraph, noting that any relevant additional information on the type of the DLT can be provided under Section 5 (additional information) of the template.

93. With respect to the various comments received regarding the description of the order and transaction, in the spirit of streamlining the template, ESMA suggests removing the following information: the way the order was placed; the person that received the order; and the means by which the order is transmitted, as in the crypto space those are not considered necessary information for NCAs’ assessment of the STOR.

94. Separately, regarding the suggestion to include under Section 3 of the template a field for the reporting entity to briefly analyse the suspicious activity and its potential impact on the market in order to help NCAs priorities their investigations, ESMA considers that

an additional field would not be needed in this case. ESMA would indeed recommend not amending Section 3 in order not to create additional burden to PPAETs and invite reporting persons to include any additional information that may be useful to NCAs under Section 5 of the template.

95. In light of the suggestion to amend the fields related to the account number, ESMA welcomes the proposals from market participants and considers that the reference to 'securities account' should be deleted. In addition, ESMA is also of the view that information on wallet address(es) involved in the transaction or suspected behaviour should be added to the template.

96. Regarding the concerns on the list of the additional information requested in Section 5, ESMA notes that the list is meant to be non-exhaustive and that only relevant/available information should be provided to NCAs within the STOR. However, for the avoidance of doubt, ESMA suggests slightly amending the description by clarifying that the list it 'indicative and not exhaustive' and that 'other information deemed useful by the reporting person may be provided where relevant to the STOR'.

97. Additionally, in relation to the specific suggestions and questions received with respect to specific fields of the draft template, it should be noted that:

- One respondent suggested that the reporting entity may not be a "person professionally arranging or executing transactions in crypto assets" and may be principally performing other roles, and therefore the header of the template should be amended. ESMA notes that the obligation to detect and report STORs, as established in MiCA, apply to the category of PPAETs, which should therefore be the target of the template. ESMA also notes that additional considerations on the scope of the obligation are presented above in Section 3 of this Final Report;

- One respondent suggested that when indicating their address, the reporting entity should specify whether it is the entity's headquarters, its registered legal address, the actual office of the reporter that is being requested, or any combination of the above. In that respect, ESMA would be of the view that such an additional piece of information should not be included in the template as this does not seem to be relevant for the purpose of assessing the STOR;

- One respondent suggested to add reference to ISO 20575 with respect to the legal form of the reporting entity. ESMA considers this information not to be needed as, when requiring the LEI of the reporting entity, ISO 20575 is automatically included in each LEI record;

- One respondent asked to provide clarity on whether CASPs operating trading platforms will be required to obtain a MIC. ESMA notes that the information on MICs is relevant as these CASPs will indeed be required to obtain one;

- With respect to the description of the crypto-asset, the same respondent mentioned that the notions of 'value' and 'right' are not clear. ESMA notes that such a wording

is derived from Article 3(5) of MiCA which defines ‘crypto-asset’ as a digital representation of a *value* or of a *right* that is able to be transferred and stored electronically using distributed ledger technology or similar technology;

- On the isolated suggestion of being more detailed in the template regarding the information specific to the DLT on which the transaction or order occurred, ESMA notes that this would likely go beyond what PPAETs can report and what is necessary to NCAs to assess the STOR. ESMA would therefore not suggest taking on board such a suggestion, also in light of the suggestions received by other respondents on the need to streamline the template on that specific section;

- Regarding the suggestion to include fields related to the interactions with smart contracts, for instance specifying the contract address and the function called, ESMA is of the view that, while useful, it would be disproportionate to include this information in the template and that, where relevant, this information can be provided either under Section 5 (additional information) of the template;

- One respondent suggested the inclusion of the LEI of the entity suspected of market abuse only when relevant to the type of transaction (i.e. in an off-chain context when such information is readily available). ESMA notes that this information is already requested on an ‘if available’ basis in the template for reporting entity and entity suspected of committing market abuse;

- With respect to the suggestion to be more specific on the taxonomy of transactions, orders and suspicious behaviours as explained in paragraph 81, ESMA is of the view that such a change would not necessary and would therefore recommend keeping the template more high-level, providing greater flexibility to PPAETs;

- In relation to the suggestion that Section 6 of the template (additional documentation) should provide a close list of documents to be included in the STOR, ESMA is of the view that the template should be kept as flexible as possible and that document should be attached at the discretion of the reporting entity;

- One stakeholder found the wording unclear regarding “media comment” in Section 6 of the template as this does not specify whether this means comment by external media, or comment on any media attached. ESMA confirms that this refers to comments by media and this is reflected in the revised template;

- One respondent suggested using a machine-readable format for submitting STORs using XBRL but ESMA notes that there is no such a requirement in Level 1 for using this format;

- One respondent stressed that ESMA should clarify that a "best effort approach" is sufficient for filling out the template and that CASPs should have more flexibility to not to include certain items. ESMA notes that this is already the case for certain fields which ESMA considers needed only when available and known.

98. Lastly, regarding the specific element of the 'location' as included in the draft STOR template shared during the consultation, 'location' of where the order is given and where the behaviour related to the functioning of DLT occurs are both already denoted as 'if available' (only the location of order execution is mandatory). Therefore, ESMA does not consider any changes based on consultation feedback as necessary. In particular, ESMA rejects the suggestion to make the entire 'location' data field based on a best-effort by PPAETs (i.e., 'where available') because it may complicate efforts by competent authorities receiving the STORs to establish a primary jurisdiction from which to pursue investigation and enforcement activities.

5 Coordination procedures between the relevant competent authorities for the detection and sanctioning of market abuse in case of cross-border situations

5.1 Proposal in the CP

99. With respect to the part of the mandate dealing with coordination procedures between competent authorities, ESMA used as starting point Commission Implementing Regulation 2020/1406 developed under MAR as this addresses the cooperation procedures, unsolicited cooperation or exchange of information, or the restrictions and permissible uses of information between competent authorities.

100. More generally, the draft RTS presented by ESMA in the CP:

- Provided a non-exhaustive list of cases that would constitute cross-border market abuse as this concept is not defined under MiCA;
- Provided for an efficient coordination procedure for the detection of cross-border market abuse, in particular by requiring a timely exchange of information that ensures that all the NCAs potentially involved have all the elements to decide whether or not to pursue a potential investigation;
- Specified the procedure, timing and form for the exchange of STORs between competent authorities and cross-referred to the template for unsolicited exchange of information set out in the ITS under Article 95(11) of MiCA for such purpose;
- Included some provisions, in line with the mandate in Article 92(2) of MiCA, regarding coordination procedures for sanctioning of those forms of market abuse. In particular, competent authorities should report the status of preliminary assessments to any other competent authorities concerned in case of (suspected) cross-border market abuse cases and these NCAs should update each other and coordinate their supervisory actions;
- Required competent authorities to inform other NCAs involved of the start of an investigation, enforcement activity or criminal investigation and may also inform

ESMA thereof. The draft RTS also foresees the possibility for ESMA to coordinate investigations and enforcement activity started by two or more competent authorities, when requested by any of these authorities.

5.2 Feedback from the consultation

101. While the proposals on coordination procedures were included in the CP, ESMA did not publicly consult on this element of the draft RTS considering that it only concerns procedures between competent authorities and does not affect market participants. Nevertheless, ESMA requested the advice of the SMSG, who made the following suggestions.

102. Firstly, the SMSG suggested specifying under Article 11(a) of the draft RTS a precise timing for the exchange of information when it comes to the requirement for competent authorities to report the status of the preliminary assessment to the other competent authorities concerned. According to the SMSG, this would also address an existing asymmetry in the draft RTS whereby, on the contrary, the receiving competent authorities shall share information about the existence of any supervisory activity or criminal investigation on the same case “without undue delay”.

103. Secondly, as opposed to the approach put forward in the CP whereby ESMA *may* be informed of the start of an investigation or an enforcement activity, the SMSG considered that ESMA should always be informed in order to have a comprehensive view of the ongoing market abuse investigations in the EU.

5.3 ESMA’s assessment and next steps

104. ESMA duly considered the feedback received from the SMSG.

105. With respect to the comment regarding the missing timing for the exchange of information under Article 11(a) of the RTS, ESMA welcomes the suggestion received from the SMSG and proposes to include the wording ‘without undue delay’ in the RTS.

106. Regarding the second point raised by the SMSG on the information of the start of an investigation or enforcement activity to be systematically conveyed to ESMA, while NCAs can activate ESMA’s coordination powers foreseen under MiCA, ESMA notes that the legal text does not set out any power for ESMA to be involved in a cross-border case without an explicit request from any of the NCAs concerned. Against this background, ESMA would maintain the wording *may* in the draft RTS as the legal basis would not justify the addition of a requirement for NCAs to systematically report this information to ESMA.

107. Finally, it is worth clarifying that a competent authority may receive STORs in its own national language referring to a potential abusive behaviour in another EU jurisdiction or which may be of interest for NCAs in other jurisdictions. In these cases, and consistent with the regular practice for the exchange of STORs under MAR, ESMA

notes that the RTS sets out that the STOR should be transmitted using the form for provision of unsolicited exchange of information under Annex IV of Commission Implementing Regulation 2024/2545[11], which provides for the possibility to include additional information such as a summary or description of the STOR.

6 Annexes

6.1 Annex I: Cost benefit analysis

Impact of the draft RTS under Article 92(2) of MiCA

108. As per Article 10(1) of Regulation (EU) No 1095/2010, all draft regulatory technical standards developed by ESMA shall be accompanied by an analysis of "the potential costs and benefits". To fulfil that requirement for this mandate with a more precise accounting of those potential costs, ESMA asked stakeholders directly in the consultation for their actual or estimated expenses associated with their current or planned market surveillance activities.

109. In this section, ESMA presents the results of our cost-benefit analysis, including the main policy options considered for the draft RTS. The results are based on ESMA's internal analysis and direct input from stakeholders in the consultation for the requirements of the RTS on the detection and prevention of market abuse (STORs). [12]

Problem identification

110. MiCA introduces a general obligation for PPAETs to detect and prevent market abuse without specifying how these entities should comply with the obligation from an organisational and governance perspective. Without a well-defined set of standards that all PPAETs should follow to adequately monitor and report suspected market abuse (beyond the generic proportionality principle), it is possible that the quality of surveillance by PPAETs would vary, exposing some investors to weaker market abuse protections.

111. Although MiCA requires PPAETs to transmit STORs to their competent authorities, there is no specification of the exact information that should be included in those reports, including when the suspected abuse is related to the functioning of the distributed ledger. In the absence of a standardised template for the information to be included in a STOR, PPAETs may not provide the best information (or enough information) necessary for competent authorities to pursue further actions in relation to a STOR.

112. Finally, given the cross-border nature of crypto markets and the likelihood that many PPAETs will passport crypto-asset services to other Member States, it is likely

[11] OJ L, 2024/2545, 26.11.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2545/oj
[12] Note that most of the actual costs stem from Level 1 obligations, which we are including here for the sake of completeness.

that competent authorities encounter evidence of market abuse that requires intensive cooperation to investigate and, if necessary, pursue enforcement. The scenarios in which cooperation among the concerned competent authorities would be necessary are not provided in MiCA, nor are the specific procedures they should follow to facilitate that cooperation.

Policy objectives

113. The objective of this draft RTS is to specify the three elements set out in the mandate in Article 92 of MiCA. These elements include: (1) the measures to ensure PPAETs have adequate governance arrangements and systems in place to detect and prevent market abuse, (2) a functional template that PPAETs should use when preparing STORs to be submitted to their NCAs, and (3) how NCAs should coordinate to investigate suspected market abuse when that abuse is found to have a cross-border dimension.

114. In light of this triple objective, the policy choices made by ESMA in the draft RTS reflect a balance between ensuring PPAETs and NCAs have all the information they require to comply with the obligation in Article 92, while maintaining efficient procedures to do so and avoiding excessive burden for the PPAETs. For detection and prevention, the requirements of PPAETs for the maintenance of systems and procedures should be commensurate with their size and scale (see Article 2(3)(a) of the RTS). The STOR template foresees that some information, especially as it relates to the functioning of the distributed ledger, may not be readily accessible to PPAETs. For cooperation between authorities, the paramount policy objective is to limit unnecessary oversharing and clarify which authority should have the ultimate prerogative in executing investigations and enforcement actions in a case involving cross-border market abuse.

115. To achieve a level playing field, ESMA started with the same STOR template used for the traditional financial sector under MAR and adapted it for crypto-specific information when suspected abuses involve the functioning of a distributed ledger. This approach means procedures for reporting suspected market abuse will be similar between the two market sectors (and hence easily comprehensible for competent authorities), except when the specific nature of crypto-asset markets demands additional or alternative information based on new standards (e.g., DTIs instead of ISINs).

Baseline scenario

116. In the baseline scenario, PPAETs would be subject to the relevant governance obligations outlined in Article 92 of MiCA with no further specification of how they should implement and comply with those measures. The result of this would be disparity in the levels of rigour of compliance with the market abuse mitigation requirements among PPAETs, especially in the absence of specifications for ensuring due proportionality of application of the requirements in the draft RTS.

117. In the crypto market today, some crypto-assets service providers are subject to market abuse monitoring obligations of varying degrees of rigour depending on the national applicable frameworks under which they are subject. However, even those Member States who have instituted national regimes for the provision of crypto-asset services do not have rules in place for the prevention and detection of market abuse that would be commensurate with MiCA obligations. As such, in the baseline scenario, it is unlikely that any of the entities currently providing regulated crypto-asset services to EU clients have introduced rigorous measures for mitigating market abuse (unless they've implemented such measures on their own initiative).

Options considered and preferred options

Policy issue 1: Use of third-party market surveillance solutions

118. ESMA considered three policy options:

- **Option 2a**: Allow PPAETs to outsource the obligation in accordance with Article 3(4) to a third-party provider of market surveillance solutions for the purposes of detecting market abuse.
- **Option 2b**: Allow PPAETs to outsource this obligation only to an in-group entity.
- **Option 2c**: Require the PPAET to use in-house capabilities and staff for market surveillance.

119. ESMA included both options 2a and 2b in Article 3(4) of the draft RTS. While PPAETs can benefit from the specialised expertise and scalability of solutions provided by third-parties or in-group entities, they also bear the costs of maintaining proper outsourcing controls. However, these costs derive almost entirely from MiCA governance requirements and DORA obligations for third-party risk management.

Costs

120. Delegating critical tasks like data analysis and alert generation introduces risks of data breaches or misuse. PPAETs will need to conduct due diligence to ensure the surveillance service provider has the appropriate expertise and solutions to meet the obligations in the regulation. This process may require background checks, audits, and regular reviews. However, as discussed, the costs of this oversight would be associated with the PPAET's compliance with general risk management obligations for outsourcing to third-party providers in the basic act of MiCA and in DORA.

Benefits

121. Instead of building costly in-house teams or systems from scratch, PPAETs can rely on a surveillance solution provider's existing infrastructure and expertise.

122. Third-party providers may offer advanced analytics tools and software for monitoring and data analysis, which could enhance the quality of alerts and detection mechanisms. By engaging with a third party or another entity in the same group, the delegating PPAET can also gain access to broader expertise and insights on market behaviour and abuse trends, benefiting from the provider's experience and specialised skills.

Policy issue 2: Human analysis of automated alerts

123. ESMA considered two policy options:

- **Option 3a**: Require human analysis of suspicious activity alerts that are generated by automated processes.
- **Option 3b**: Allow for a completely automated process in which a software generates alerts and generates STORs without a human in the loop.

124. ESMA has selected option 3a. Although human analysis would create some operational burdens for PPAETs, such burden would not be disproportionate for the purposes of market abuse detection and would enable NCAs to start their evaluation of possible market abuse cases from more reliable STORs.

Costs

125. Costs would derive from the operational expenses incurred from staffing and training by PPAETs to review suspicious transaction alerts for their relevance. As compliance staff would already be required under the governance arrangements (to prepare and submit STORs), it is unlikely that this requirement in the draft RTS would necessarily incur *additional* costs (although this would depend on the PPAETs volume of transactions and alerts generated).

126. Introducing a layer of human analysis might lengthen STOR processing times. This may cause inefficiencies, especially considering the algorithmic and high-frequency trading.

Benefits

127. Human analysis is necessary to identify if a suspicious transaction requires further evaluation to confirm whether it is relevant or consistent with a pattern of behaviour that would constitute abuse. Requiring this analysis of PPAETs would prevent them from passing the burden entirely onto NCAs receiving the STORs—a suboptimal outcome considering those PPAETs would be in a better position to determine the relevance of an alert and whether it should be submitted in the first place.

128. Some forms of market abuse, particularly in markets for crypto-assets, may be too subtle or complex to be identified by fully automated systems. Human analysts can recognise patterns and adapt the models used for detection, ensuring better

responsiveness to emerging threats. Automation can also lead to high rates of false positives in identifying suspicious transactions. Human analysis can be used to fine-tune the results produced by automated detection systems, reducing unnecessary alerts and focusing on real risks.

Policy issue 3: Timing of submission of STORs and information in the template to be provided on a 'best effort basis'

129. ESMA considered two policy options:

- **Option 1a**: One-time STOR submission with all the information that a competent authority may require to pursue an investigation, including optional information provided on a 'best effort' basis.

- **Option 1b**: A 'two-track' STOR submission process in which the PPAET would submit a 'streamlined' STOR to their competent authority with only essential information (to shorten STOR processing times). The PPAET could then follow up this initial submission with additional detail at the request of the competent authority.

130. ESMA opted for option 1a because the adequate level of detail required at the time of initial submission of a STOR is crucial for ensuring effective market abuse detection and enforcement.

Costs

131. Once a STOR is submitted, it cannot be updated or revised if additional information becomes available. With no option to 'revise' a STOR, PPAETs may simply resubmit them (causing overreporting) or the include irrelevant details, reducing the clarity and focus of the STOR. However, there are already some mitigating circumstances in the draft RTS which allow for iteration in the sharing of information between PPAETs and NCAs. Article 6(3) of the draft RTS foresees the ability of PPAETs to follow up with the competent authorities with 'any relevant additional information which they become aware of after the STOR has been originally submitted' and 'provide any information…requested by the competent authority'. The possibility to submit STORs 'without delay' in Article 6(1) of the draft RTS instead of within a defined timeframe also gives PPAETs sufficient flexibility to decide for themselves when they have sufficient information to submit a 'complete' STOR.

132. A single STOR template combining mandatory and 'best effort' data fields could cause slower processing times than a two-track process from the point of the generation of an alert to the submission to the competent authority. This potential for delay could hinder the speed and efficiency of follow up actions by the NCA.

Benefits

133. A one-time submission encourages PPAETs to standardise their internal data-gathering processes, leading to more consistent, complete reports. It also helps to eliminates the need for authorities to frequently request additional information from the PPAETs. Further, the possibility to provide some information on a ‘best effort’ basis recognises that data extraction, especially in the on-chain context, can be more complex and time-consuming than data collection involving a PPAETs own ICT systems.

134. In the case of a two-track submission as provided in option 1b, if essential information is missing from the initial STOR, authorities may not have enough data to act quickly, delaying potential market abuse investigations. The lag between initial and supplemental submissions could undermine timely enforcement. The benefit of a one-time submission per option 1a is the lower likelihood of delays due to incomplete information.

Stakeholder groups affected	Costs	Benefits
Persons professionally arranging or executing transactions (PPAETs)	The costs stemming directly from the measures specifying MiCA requirements found in the draft RTS are: **Record-keeping**: The requirement to identify and keep a five-year record of information related to the analysis of alerts generated, including near-misses, is a key one-off and on-going cost driver. **Training**: The relevant staff of the PPAET is to be trained on an ongoing basis to ensure an 'appropriate level of human analysis'. Indeed, to ensure that staff have a good understanding of what suspicious activities look like, they should be properly trained to identify the conduct that does not meet the threshold for a STOR submission but should nevertheless be recorded for further assessment in case of repeated behaviour. **Proportionality**: The draft RTS requirements provide that PPAETs' systems and procedures should be appropriate and proportionate in relation to the scale, size and nature of their business activity. In that sense, the draft RTS ensures that smaller PPAETs will bear lower costs relative to bigger players.	By specifying that PPAETs maintain a five-year record of their analyses of automated alerts, the RTS would enhance detection of repeat cases of market abuse, which NCAs would also be able to reference in future supervisory actions. Mandating training of PPAET staff for the analysis of alerts improves the quality of STOR submissions, enhancing investor confidence, and reducing the risk of regulatory enforcement actions for PPAETs. Additionally, by allowing PPAETs' systems and procedures to be appropriate and proportionate in relation to the scale, size and nature of their business activity, the draft RTS will aim at promoting competition between PPAETs. On the same line, allowing the production of alerts (and building of surveillance tools) to be outsourced to a third-party provider will ease the burden on SMEs for whom developing an internal solution would be too complex and expensive. A standardised template for reporting STORs will facilitate PPAETs' compliance with the MiCA regime, by making clear the appropriate level of information and promote a consistent application of the reporting duties across the EU.

Stakeholder groups affected	Costs	Benefits
	Costs for PPAET related to the detection and prevention of market abuse are also derived from the application of requirements in Article 92 of MiCA—not specifically derived from this draft RTS. This would include software licensing costs and annual audits (internal or external) of the systems, arrangements and procedures of PPAETs.	
Competent authorities	L2-related costs for competent authorities are likely to be relatively minor. Competent authorities may incur in some training costs for staff in charge of assessing the received STORs, but that is directly connected with the MiCA obligations.	The RTS will clarify the expectations for market abuse prevention in the crypto-asset market. This will help firms to develop appropriate compliance programs and reduce the need for enforcement actions by supervisors. The template for reporting STORs included in the draft RTS will also facilitate the analysis of the information reported by the NCAs and will promote efficient information sharing in case of cross-border investigations. Adequate systems and procedures for the prevention of market abuse will also avoid overreporting of STORs, which can be burdensome for NCAs and hence counterproductive to robust enforcement against crypto-asset market abuse. Differently, fewer but higher quality STORs will facilitate NCAs assessment and reduce the amount of resources they need to that purpose.
Other stakeholders	While none of the respondents to the consultation cited this as a possible outcome, some of the costs may be passed on to clients	The implementation of market abuse detection and prevention systems ensures a higher level of market integrity, promoting markets in crypto assets with reduced risk of

Stakeholder groups affected	Costs	Benefits
	by PPAETs through commissions on the services they are providing.	manipulation, insider trading, and other fraudulent activities. This protects clients from being disadvantaged by unfair practices. When clients know that market abuse is being actively monitored and addressed, they can have more confidence that their transactions are fair, and their investments are secure.

6.2 Annex II: Question by question feedback from the consultation

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

ESMA received 28 replies to this question.

The answers can be grouped around three main issues.

The vast majority of responses (18) considered that **miners and validators** should not be considered within the scope of PPAETs, providing a wide range of reasons for that. Whereas most of these responses considered that the role of miners/validators is equivalent to that of IT or telecom providers, one stakeholder assimilated them to the "settlement service" of the transactions in crypto-assets. Moreover, some of these stakeholders considered that including them within the scope of PPAETs would create two types of risk: de-localisation of European miners/validators to other jurisdictions and stifling innovation in EU markets.

Two respondents distinguished between the blockchain networks, noting that each decentralised blockchain network processing, ordering and finalising user transaction can differ. Therefore, instead of a general assumption regarding the role of miners/validators as PPAETs (or a general assumption in the opposite direction), they recommend analysing their role and in particular whether they have the capacity to rearrange the order of the pending transactions. These responses underlined:

- That reordering transactions within a PoW system would disrupt the continuity of the blockchain and lead to inconsistencies in the transaction history i.e. to invalid blocks.

- In PoS, validators are typically blind to the content of the transactions before they are included in a block. This blind validation prevents them from selectively reordering transactions.

- Validators outsource the block building to external searchers, builders and relays in the Ethereum market structure. Under this scheme, validators do not have the capacity to modify the order of the pending transactions, which is arranged by searchers and builders. Therefore, these responses recommend considering searchers and builders as PPAETs.

In relation to this point, fourteen respondents reacted against mechanically assuming that **Maximum Extractable Value (MEV)** is always market abuse. These responses noted that MEV refers to the value that can be extracted from block production in addition to the standard gas fees, by including, excluding, or ordering transactions within a block. For these stakeholders, MEV's primary purpose is to compensate good actors for the work performed, providing incentives to validators. This is achieved by the capacity of users to facilitate the

execution of their transaction in front of others simply by increasing the gas fees they are willing to pay for a transaction.

For these respondents, whilst some types of MEV are inherently abusive (the so-called sandwich attacks, time-bandit attacks or using inside information from private mempools), other types of MEV are a legitimate practice, facilitating arbitrage across decentralized exchanges or identifying opportunities to liquidate DeFi positions. However, these same respondents acknowledged that the analysis of MEV is still at an early stage and mentioned some academic and regulatory articles identifying sound practices.

Likewise, most of the responses received (15) considered that CASPs providing solely the service of **safekeeping and administration of crypto-assets** should not be considered as PPAETs. These respondents' main arguments were based on the proportionality principle, since the CASPs solely offering these services do not manage or execute transactions. In line with that, these entities may not have the necessary internal controls or the access to the information necessary to detect abusive behaviour. In particular, one reply noted that CASPs providing custody where the private keys are in control of the client lack all the operational capabilities of the client.

Some of these responses highlighted that CASPs providing other services listed in the CP should be included within the scope of PPAETs. One reply expressed against including custodians and depositories as PPAETs by default. Instead, they proposed a case-by-case assessment of the operating model.

However, it is worth noting more nuanced or diverging responses:

- Three respondents raised the need for clarifying whether CASPs offering only transfers of crypto-assets should be considered as PPAETs. These responses noted that Article 1 of the RTS on record-keeping by CASPs included within the definition of "executing a transaction" "transfer of crypto assets to or from accounts". One of these responses provided the following elements supporting the exclusion of the transfer of crypto-assets from one account to another: i) the mere transfer does not give rise to market abuse practices; and ii) it is challenging to conceive how a CASP solely providing this service could identify reportable behaviour. One custodian considered that an important reason to maintain custodians and depositories out of the scope of PPAETs is that MiCA considers stable-coins as crypto-assets and it is to be anticipated that as part of many administration processes CASPs will exchange stable-coins for fiat currents and/or for other stable-coins.

- Three stakeholders considered that custody and administration should be within the scope of PPAETs, due to their direct involvement with clients' assets and potential impact on market integrity. According to one of these responses, the custodians of digital assets hold significant influence over the digital assets they manage, including control over the transactional processes.

One respondent, when answering the following question, considered that CASPs operating a trading platform should not be assimilated to PPAETs and therefore, should be excluded from

the scope of the RTS. One association considered that alternative investment fund managers should be excluded from the scope of PPAETs because they are not directly involved in the management of the fund but outsource it externally.

One response considered that the STOR template was not proportionate and demanded a regulatory grace period to ensure that market participants can adapt to the new regulatory environment. One association recommended maintaining the STOR template as aligned to the MAR one as possible and revise it at a later stage.

Some responses requested a clarification of terms mentioned in Level 1, such as “admitted to trading” (Article 86 MiCA) and “other aspects of the functioning of the distributed ledger technology such as the consensus mechanism” (Article 92 MiCA).

Finally, some responses raised the new types of market manipulation and fraud that may arise in decentralised networks, such as conflicts of interest between service providers involved in MEV activities (validators, searchers, builders). Other replies noted that certain types of market manipulation do not take place in the DeFi environment (“trash&cash”, “marking the open” and “marking the close”).

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.

ESMA received 21 replies to this question.

The respondents were almost unanimously supportive for the proposed RTS with a number of comments or proposals.

The main issue arising from the comments received is related to the proportionality principle and how should it be applied in the context of crypto-asset markets (ten responses).

Several responses questioned whether CASPs should monitor off-chain transactions and how should “other aspects of the functioning of the distributed ledger technology” be monitored. Three responses supported that CASPs should monitor off-chain and on-chain data, whereas a number of respondents expressed against such requirement. For them, this requirement was not proportionate. One of the supporters of monitoring off-chain data noted that the integration of both data sets is complex because the execution and settlement of on-chain transactions may take minutes up to one hour. Four additional responses reiterated that MEV should not be mechanically assimilated to market abuse and therefore, PPAETs should not be obliged to report all instances of MEV identified.

The impact of the requirements for small companies was addressed from different perspectives:

- Several responses considered that the scope of the monitoring activity should be better framed, excluding “aspects of the distributed ledger

technology" or on-chain transactions after they leave the environment of the executing entity.

- Other responses considered that given the implementation costs of in-house surveillance systems it should be possible to outsource these systems; flexibility in the periodicity of periodic reviews (that should be 18 months for SMEs whereas large firms should undertake them every 12 months).

As opposed to that, some responses proposed setting a "minimum common denominator" applicable to all PPAETs including:

- One venue considered that in PPAETs should have in all cases real-time or near-real time monitoring; in-house or third-party surveillance software (tested, capable of identifying all relevant abusive trading and periodically reviewed); adequately staffed; it should include monitoring for employee insider trading; and annual review of market abuse risk.

- Data generation and retention (timestamp and prices) (two responses)

- Trade surveillance risk scoring should be integrated into CASPs' risk scoring (two responses)

- Trade surveillance systems should be calibrated according to the asset and liquidity profile of the instrument, customer segment and the type of trading activity to avoid "false positives" (two responses). Another stakeholder considered that Article 8 of the draft RTS should impose the obligation to monitor not only orders and transactions but also price and volume movements, order book imbalances and social media activity.

- It is worth noting that another reply considered necessary to define in Article 10 of the RTS the type of alerts that should be generated, the threshold for triggering alerts and the escalation procedures for investigating those alerts.

A number of clarifications/proposals in relation to MiCA and the draft RTS were requested:

- Several responses raised questions in relation to Article 2 of the draft RTS: how should trading platforms apply the requirement of monitoring irrespective of "whether the orders were placed or transactions executed on or outside a trading platform"; whether CASPs should monitor the entire market or just the exchanges they operate.

- One respondent requested a clarification of what should be considered as market abuse "likely to be committed" and about the human analysis reflected in Article 5.

- Three responses asked for further specification of the timing of submission of STORs in Article 6.

- Another response noted that the industry and regulators should cooperate to specify in which territory or jurisdiction an asset is traded, because the parameters to consider for that purpose are not shared with traditional finance.

Three replies considered that despite the reference to “algorithmic trading” in Article 3, the RTS should be technology-neutral and remain applicable to an evolving trading environment, where Artificial Intelligence and machine learning are increasingly present.

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

ESMA received 21 replies to this question.

Respondents provided different suggestions with respect to the draft template presented in the CP. The feedback is presented section by section.

With respect to Section 1 of the template (identity of the entity/person submitting the STOR), ESMA received the following comments:

- One respondent suggested that the reporter may not be a “person professionally arranging or executing transactions in crypto assets” and may be principally performing other roles and to adjust the sub-header in the template.

- One respondent suggested that the information on legal form of the reporting entity should be requested using ISO 20575.

- One respondent suggested that when indicating their address, the reporting entity should specify whether it is the entity’s headquarters, its registered legal address, the actual office of the reporter that is being requested, or any combination of the above.

- One respondent suggested that when indicating the type of trading activity, this should also indicate whether the suspicious activity is a regular activity of the reporting entity or solely that related to the suspicious activity (if any).

With respect to Section 2 (Transaction/order/behaviour and other aspect related to the functioning of the Distributed Ledger Technology), ESMA received the following comments:

- Five respondents raised concerns with respect to the field requiring the description of the distributed ledger. In particular:

  – One stakeholder suggested that this item is redundant if a Digital Token Identifier (DTI) is already provided in the template;

- A few respondents considered that ESMA should at least eliminate requirements to report publicly available information such as the description of the functioning of the DLT. The rationale behind such a choice is not to request too much information in order not to decrease quality of reporting;

- One stakeholder stressed that some aspects of the DLT like consensus mechanisms may be difficult to assess as some firms may not have the technological capacity to access;

- One stakeholder considered that the description of DLT ledger should not be included as this is too technical and in other sectors technical details are not required. The same respondent suggested that, in case this is kept, it should be strictly minimised to the simple information about the type of DLT/blockchain network (e.g. name).

- This view was not shared by one respondent who, on the contrary, suggested being more detailed on the information specific to the DLT on which the transaction or order occurred. In the respondent's view, this could include the blockchain name, the block number, and the transaction hash. In addition, the same respondent suggested that the template should include options for specifying suspicious behaviors related to the DLT's functioning (e.g., front-running, transaction reordering, consensus mechanism manipulation).

- Two respondents suggested distinguishing between private/public blockchain. In addition, they considered that the fact that ESMA does not refer to the consensus mechanism but rather to the type of the distributed ledger can create some logistical issues on whether CASPs must report market abuse regarding permissioned DLTs;

- With respect to the description of the order, one respondent suggested that some fields may not be applicable depending on the nature of the suspicious activity (e.g., settlement date and time as "Transactions designed to fail won't have a settlement").

- One respondent raised concerns about the amount of information requested under section 2 and in particular in relation to the name and MIC of the trading platform, the LEI of the CASP carting out the transactions, the location, the DLT, details on the DLT, etc, and explained that this is more burdensome than the template under MAR; On the issue of the MIC, the same market participant requested clarifications on the meaning of MIC, as it is not clear whether the trading platforms will be obligated to get the MIC.

- This same respondent also mentioned, with respect to the description of the crypto-asset, that the notion of 'value' is not clear, as it is unclear whether this refers to the value involved in the transaction at the time of transacting or to a unit value per crypto-asset involved and that the notion of 'right' is also not clear, as it is unclear what right the token holder has at this stage of market abuse and in terms of the reporting obligation;

- Another respondent indicated that some of the fields related to order submission are unclear: “way” and “means” the order was placed (same comment reiterated by another respondent); it’s unlikely it will be a “person” receiving the order;

- Along the same line, two stakeholders stressed that fields on “the person that actually received the order” and” the means by which the order is transmitted” might be difficult (or practically impossible) to access and therefore should be flagged under the condition “if applicable and known”;

- Regarding the ‘location’ of the order/trade/behaviour, three respondents considered that this is irrelevant for DLT due to the decentralised nature of the network and the use of IP masking techniques like VPNs.

- Two stakeholders suggested to add information on unique identifier of the transactions on the blockchain (e.g., ticker symbol, contract address) to facilitate accurate identification and tracking.

With respect to Section 3 (Description of the nature of the suspicion), ESMA received the following comment:

- One respondent suggested that the template could include an optional field for the reporting entity to briefly analyze the suspicious activity and its potential impact on the market in order to help NCAs in prioritising their investigations.

With respect to Section 4 (Identification of the person(s) responsible for the orders, transactions or behaviours related to the functioning of the Distributed Ledger Technology that could constitute market abuse (‘suspected person’), ESMA received the following comments:

- One stakeholder raised concerns in relation to the field “Account number”, as this is named as a securities account whereas it should be named as a crypto-asset account, and in addition its number is likely to be the identifier meaning the public address in the distributed ledger or in the smart contract;

- One respondent suggested adding the LEI (Legal entity identifier) of the reporting entity of the transaction;

- One respondent expressed concerns on the information requested under this section such as National Identification Number (NIN) or number of account which may not be available to the PPAET.

- One respondent considered that the template should include fields for recording the use of protocol-level safeguards like threshold encrypted mempools, which can significantly aid in the detection and prevention of market abuse;

With respect to Section 5 (Additional information), ESMA received the following comments:

- One stakeholder considered the term “trading desk” to be unclear as most crypto asset activity is software-automated and not associated with a “desk” as in traditional financial activity;

- One respondent voiced concerns on the list of the additional information requested (e.g. trading pattern) mentioning that this could entail an additional cost to reporting entities.

With respect to Section 6 (Documentation attached), ESMA received the following comments:

- One respondent recommended that the template should explicitly state the types of supporting documentation that would be most helpful for NCAs in their investigations. This could include order book data, transaction logs, communication records, and social media posts.

- One respondent suggested that ESMA should provide examples of the supporting documentation and materials, including templates, that should be provided with the STOR.

- One stakeholder found the wording unclear regarding “media comment” as it does not specify whether this means comment BY external media, or comment ON any media attached?

Lastly, some respondents also made the following general comments and suggestions:

- A few respondents considered that the template contains too much information, more than necessary to identify market abuse. It was therefore recommended that ESMA should streamline the STOR template to ensure that CASPs are able to quickly report enough information to allow NCAs to act upon the STOR. One stakeholder also suggested that ESMA expressly delineates what information is critical and required to be provided with each initial filing and that additional information could be provided where needed, at a later stage in order to favour a more timely and swift submission of STORs without the need of gathering unnecessary information.

  According to these market participants, examples of unnecessary information in the STOR template is the description of the crypto-asset and a description of the DLT as this information is publicly available and already known by NCAs for assets that are trading within their regulatory framework. In one respondent’s view, other examples of information to be removed are those related to the DoB, DTI, LEI of the CASP, full address information of underlying client (person or entity) Information about the employment of the underlying client (person or entity) and account number.

- One respondent recommended implementing of a dedicated portal making any declaration easier and homogeneous for the declarants;

- One respondent suggested using a machine-readable format for submitting STORs using XBRL;

- One respondent recommended including clear definitions for any technical terms used in the template, especially those related to DLT as this would ensure a common understanding among all stakeholders and clear limits to the scope of requirements.

- A few respondents raised the issue of the confidentiality of the information requested. In particular, as several items of information requested, such as National Insurance Number, are generally treated as sensitive, there should be reassurance that supplying NINs will not constitute a violation of GDPR. Furthermore, one of these stakeholders considered that the identity of the suspected person (name, national identification number, address, date of birth, account numbers and information about employment, etc) should be not automatically reported to the NCA until reasonable suspicion has been confirmed and it has been established that the reported transaction is indeed malicious and/or constitutes market abuse.

- One respondent stressed that ESMA should clarify that a "best effort approach" is sufficient for filling out the template and that CASPs should have more flexibility to not to include certain items, or that those could be included at later stage.

- One respondent highlighted that it is not clear why the name of the person in charge of the reporting should be included and that instead this should only refer to the contact or to the name of the person assigned within the company as the point of contact for the authority;

- One respondent considered that ESMA should develop further guidance, including Q&A, to support CASPs and other PPAETs when completing and submitting STORs.

- One respondent provided a suggestion whereby reporting persons should receive annual feedback on the quality of the STORs submitted in the same way that the NCAs currently do with the SARs (Suspicious Activity Reporting) that the CASPs submit.

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?

ESMA received 21 replies to this question.

Respondents did not identify any parameters/naming convention that would substantially alter the template but made the following suggestions:

- One respondent recommended including parameters indicating whether a transaction passed through an encrypted mempool or similar mechanism would be beneficial as this could help identify patterns consistent with front-running or MEV;

- One respondent suggested including a field for specifying the wallet addresses involved in the transaction as this would help identify suspicious activity patterns across different wallets and link them to specific individuals or entities.

- One respondent suggested that ESMA should develop a taxonomy to define the parameters and naming conventions for the submission of crypto-asset related STOR templates. For instance, a ‘transaction types’ taxonomy could include ‘swap’, ‘transfer’ and a ‘suspicious behaviours’ taxonomy could include ‘rug pulls’, ‘oracle manipulation’ and ‘pump-and-dump’. The last part of this comments was supported by some stakeholder who considered that the list of suspicious behaviours should be more detailed and expanded to include specific conducts such as wash trading, rug pulls, pump and dumb, spoofing, oracle manipulation, etc.

- Another respondent considered that there should be more detailed as to order types in order to include options for "Market Order," "Limit Order," and "Stop-Loss Order," as these are common order types in both traditional and crypto-asset markets and to include options for “Stop-Gain Order”, for the same reasons;

- One respondent stressed that while naming conventions in the template itself are appropriate and do not need to be modified, ESMA should significantly streamline the list of parameters in the template;

- Lastly, to ensure that the regime is effective, a few respondents suggested that 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.

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?

ESMA received 20 replies to this question.

Almost all respondents expressed scepticism about the practicalities of identifying the geographic location of a validating node or miner in a permissionless DLT network, confirming the common practice of masking IP addresses by use of a VPN. Indeed, several respondents noted that in most cases, DLT operators are not aware of the geographic location of the (legal or natural) persons operating nodes on their own networks. As such, they requested that ESMA maintain the voluntary nature of the ‘location’ field in the STOR template (i.e., *if available*).

Several respondents acknowledged the availability of a physical location (country) for cases where participating nodes must register or be identified by a central entity responsible for operating and maintaining the DLT network. Even further, one respondent acknowledged the importance of this data point for regulators as it relates to establishing a legal jurisdiction when the suspected market abuse involves a node contributing to the consensus mechanism of a DLT.

But many respondents questioned the utility of identifying node locations for the purposes of STORs. For example, one respondent said there is no utility in requiring the location of a node in the template because nodes do not initiate transactions (they only decide whether to bid on

rights to mine/validate a block). As such, the location of the actual node responsible for executing the transaction may be immaterial to the suspected market abuse.

Only one respondent offered (conditional) support for the inclusion of location in the template with the caveat that ESMA should not require PPAETs to go beyond what is stated in the template (i.e., provide location where it is available). For example, PPAETs should not be responsible for employing advanced technical resources to “unmask” an IP address or geolocate a node in cases where a VPN is used (to avoid additional burden on these reporting entities).

A workaround option proposed by one respondent was to simply require the public address of the node (unique numbers that serve to identify the node on the DLT network). Otherwise, another point of control would be to identify the location of the servers on which a node stores off-chain (if available).

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.

ESMA received 16 replies to this question.

With respect to other element or information relevant to crypto-asset markets that should be included in the template, respondents made the following suggestions:

- Include NFTs to the crypto-assets covered;
- Three respondents considered that information on interactions with smart contracts could be included, as these can significantly influence market behaviour. This can for instance touch upon details regarding the execution of smart contracts, any associated events, or the calling of specific functions could provide insights into potential market manipulation or abuse;
- One respondent recommend including fields that capture the use of encryption and privacy-preserving technologies as this data can provide insights into the effectiveness of technical solutions in preventing market abuse.
- Two respondents recommended that ESMA should remove, rather than add, information from the template, requiring only the immediately available and necessary information to begin an investigation, in order to reduce the burden on reporting entity
- On the contrary, one respondent suggested including information on:
  - Wallet Addresses involved in the transaction to help link activities across different transactions and identify suspicious patterns.
  - 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.

  - Contextual Information such as prevailing market conditions, significant news events, or other external factors influencing trading behaviour.

  - Social Media Information and Activity associated with the crypto-asset or participants. This can help identify coordinated efforts to manipulate market sentiment or price.

- Similarly, another respondent suggested including information on:

  - Transaction value and volume in fiat currency and the relevant crypto asset;

  - Transaction fees associated with the transaction or order (this suggestion was also supported by another respondent);

  - Fields for identifying the counterparty to the transaction or order. This could be a wallet address, a user ID on an exchange, or any other relevant identifier.

  - The trader's recent trading history for the relevant crypto asset;

  - For transactions on public blockchains, the transaction hash and the block number;

  - If suspicious activity is detected on social media platforms, fields for specifying the platform, the relevant posts or messages, and associated user handles or accounts.

- Lastly, while not providing any real suggestion, one respondent considered reviewing how the requested information corresponds with the GDPR requirements and how this interacts with cross-border regulatory coordination.

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.

ESMA received 14 replies to this question.

Most respondents called for a proportionate approach to the obligations in the draft RTS, allowing PPAETs (particularly SMEs) to tailor their systems and procedural requirements to the capabilities and risk profile of their activities. Otherwise, smaller firms may face disproportionate costs relative to their size and resources, creating anti-competitive pressure on EU-based crypto startups.

One trade association respondent said the costs of implementing the market abuse detection tools to meet the requirements of the RTS would range between €40,000 and €300,000 annually (with software licensing costs making up the bulk of the total, i.e., anywhere between €100-250k). For most SMEs, this respondent said, developing an internal solution would be

too complex and expensive, making outsourcing a preferred option. A crypto-asset trading platform confirmed that a third-party solutions may cost approximately between €110,000 - €130,000 per year.

In addition to the cost of the software, said the addition of new FTEs will also need to be considered for alerts handling (since the RTS requires human analysis of alerts). As many types of transactions will involve different CASPs (brokers, RTO, exchange), one respondent said the RTS should take a proportionate approach to how each of these PPAETs would share the burden in transaction monitoring.

One respondent said the costs associated with the obligations in the draft RTS can vary widely depending on the size and complexity of the operations. For medium to large firms, this could range from €50,000 to €500,000. One advantage or cost mitigator identified by respondents was the fact that many crypto-native market surveillance technologies provide free data access, unlike traditional legacy systems.

Several respondents echoed the request for a phased implementation or ‘grace period’ to allow market participants time to anticipate or defray the costs associated with compliance.

6.3 Annex III: Advice of the Securities and Markets Stakeholder Group

135. The full SMSG advice can be found on the ESMA website[13]. For reference, the relevant excerpt on the market abuse RTS is available in the box below. The ESMA response is embedded throughout the discussion provided in the explanatory text of the Final Report (i.e., Sections 3, 4, 5).

3 SMSG opinions and comments on market abuse

3.1 General approach, proportionality and riskiness in market abuse monitoring.

3. ESMA considers that the draft technical standard should require that persons professionally arranging or executing transactions (PPAETs) to establish arrangements, systems and procedures that ensure an effective and on-going monitoring of transactions, orders and other aspects of the functioning of the distributed ledger technology and allow for the reporting of suspicious transactions or orders to the relevant NCA.

4. The SMSG supports the approach put forward by ESMA to monitor market abuse, as it is a key aspect for the long-term success of the crypto ecosystem.

5. ESMA also notes that – considering that the size, nature and scale of the business activity carried out by PPAETs may vary significantly – it is important to ensure that systems, arrangements and procedures developed by PPAETs are proportionate and appropriate to comply with the STOR (i.e., suspicious transaction or order report) regime. At the same time, ESMA also considers as important that these systems and procedures are adequately calibrated to the risk dimension of the activities carried out by PPAETs.

6. Specifically, article 2.3.(a) of the draft RTS on market abuse requires that arrangements, systems and procedures "are appropriate and proportionate in relation to the scale, size and nature of their business activity".

7. The SMSG believes that this provision may imply overlooking the risk dimension of the activities carried out by PPAETs. The risk of market abuse does not depend only on the scale, size and nature of the business activity of the PPAETs. It also depends, e.g., on the interaction between the scale of the PPAETs activity and the size of the crypto-asset market. For this reason, we are of the opinion that article 2.3.(a)[14] should be amended to include that the proportionality should be allowed only when the PPAET shows – e.g., based on empirical evidence or establishing appropriate policies and procedures – that its activity does not imply risks of market abuse at a material level.

[13] ESMA. (2024, June). *SMSG advice on MiCA package*. Retrieved from https://www.esma.europa.eu/sites/default/files/2024-06/ESMA24-229244789-5075_SMSG_Advice_on_MiCA_package__3.pdf.

[14] See 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").

8. The SMSG also considers that it would be helpful to clarify whether the monitoring and detection of market abuse for cryptos requires special mechanisms and tools with respect to the mechanisms and tools usually applied to securities markets.

3.2 Outsourcing and systemic risk

9. ESMA considers that PPAETs may delegate their prevention and detection activity, including the performance of data analysis and generation of alerts, to a third party or to a person of the same group.

10. To ensure that PPAETs remain in control of those functions, the draft RTS sets out some necessary requirements, such as the existence of a written agreement between the parties and the retention of access to the relevant information and the necessary expertise so the PPAET may assess the work conducted by the delegated party.

11. Specifically, article 3.4 of the draft RTS on market abuse sets out the requirements for the outsourcing of the prevention, monitoring and detection activities.

12. The SMSG believes that the outsourcing of such sensitive tasks should also consider systemic risks (e.g., when several PPAETs delegate the same provider). The relevant authorities may need to monitor the competition and concentration levels of the market related to the outsourced activities.

3.3 Coordination procedures between competent authorities

13. With respect to the coordination procedures between competent authorities for detection and sanctioning of cross-border market abuse situation, ESMA considers that the draft technical standard should provide for an efficient coordination procedure for the detection of cross-border market abuse, in particular by requiring a timely exchange of information that ensures that all the NCAs potentially involved have all the elements to decide whether to pursue a potential investigation or not.

14. To avoid ambiguity and to foster convergence, the SMSG believes that it would be useful to specify a precise timing for the exchange of information: article 11 of the draft RTS on market abuse requires the competent authority suspecting a case of cross-border market abuse to “report the status of its preliminary assessment to the other competent authorities concerned”. However, there is no expected timing for this reporting activity to occur.

15. By contrast, the receiving competent authorities shall share information about the existence of any supervisory activity or criminal investigation on the same case “without undue delay”. It appears that an asymmetry in the expected timing exists between the NCA originating the coordination activity and the NCA receiving the preliminary assessment[15].

[15] See 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”).

16. The draft RTS also foresees the possibility that competent authorities inform ESMA of the start of an investigation or an enforcement activity. The SMSG believes that, instead of being a possibility, ESMA should always be informed in order to have a comprehensive view of the ongoing market abuse investigations in the EU. Indeed, MICA level 1 text provides good arguments to consider this as a requirement rather than as a possibility. We list such arguments in the next paragraph.

17. First, the first paragraph of Article 95(1) provides that competent authorities should cooperate with each other and render assistance to NCAs of other Member States and to EBA and ESMA. They should exchange information without undue delay and cooperate in investigation, supervision and enforcement activities. Second, the second paragraph of Article 95(1) provides that, where Member States have laid down criminal penalties for certain market abuse infringements of MiCA, they shall ensure that appropriate measures are in place so that NCAs have all the necessary powers to liaise with judicial, prosecuting or criminal justice authorities within their jurisdiction to receive specific information related to criminal investigations or proceedings commenced for infringements of MiCA and to provide the same information to other competent authorities as well as to EBA and ESMA, in order to fulfil their obligation to cooperate for the purposes of MiCA. Third, there are only limited reasons to refuse an exchange of information (see Article 95(2) of MiCA). Fourth, EBA and ESMA shall fulfil a coordination role between competent authorities and across supervisory colleges as referred to in Article 119 with a view to building a common supervisory culture and consistent supervisory practices and ensuring uniform procedures. (Article 95(8), second paragraph), providing a further argument for ESMA and EBA to be fully informed.

6.4 Annex IV: Draft RTS pursuant to Article 92(2) of MiCA

COMMISSION DELEGATED REGULATION (EU) 2024/XXX

of XXXX

supplementing Regulation (EU) 2023/1114 of the European Parliament and of the Council with regard to regulatory technical standards specifying the appropriate arrangements, systems and procedure as well as the templates to be used for preventing, detecting and reporting suspected market abuse, and on the coordination procedures between the relevant competent authorities for the detection and sanctioning of market abuse in cross-border market abuse situations

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets and amending Regulation (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937[16], and in particular Article 92 (2), third subparagraph, thereof,

Whereas:

(1) It is necessary to specify appropriate requirements for the arrangements, procedures and systems that persons professionally arranging or executing transactions in crypto-assets should have in place for the reporting of orders, transactions and other aspects of the functioning of distributed ledger technology, such as the consensus mechanism, where there might exist circumstances indicating that market abuse has been committed, is being committed or is likely to be committed. Such requirements are critical and should assist in the prevention and detection of market abuse. They should also assist in ensuring that suspicious reports concerning reasonable suspicions on orders, transactions and other aspects of the functioning of distributed ledger technology (STOR) submitted to competent authorities are meaningful, comprehensive, and useful.

(2) In order to ensure that prevention and detection of market abuse is effective, appropriate systems should be in place to monitor orders, transactions and other aspects of functioning of the distributed ledger technology, in accordance with the scale, size and nature of the business activity of the person professionally arranging or

[16] OJ L 150, 9.6.2023, p. 40.

executing transactions. Such systems should provide for human analysis carried out by appropriately trained staff. The systems for monitoring market abuse should be capable of producing alerts in line with predefined parameters in order to allow for further analysis to be conducted on potential insider dealing or market manipulation or attempted insider dealing or market manipulation. The whole process is likely to require some level of automation.

(3) The analysis of the appropriateness of the arrangements, systems and procedures should include the assessment of the impact that the person professionally arranging or executing transactions may have on the market. As part of that assessment, a person professionally arranging or executing transactions should consider whether they have a significant or dominant position in any crypto-asset market asset segment. In that case, its arrangements, systems and procedures to prevent and detect market abuse should be proportionate to its enhanced influence in the market.

(4) The prevention and detection of market abuse includes the ongoing monitoring of all orders and transactions arranged or executed by the persons professionally arranging or executing transactions, irrespective of whether they are executed on the distributed ledger ('on-chain') or outside the distributed ledger ('off-chain'), including transfer of crypto assets to or from accounts of clients of the same crypto-asset service provider.

(5) In order to facilitate and promote a consistent approach and practices across the Union in relation to prevention, detection and sanctioning of market abuse, it is appropriate to lay down detailed provisions harmonising the content of, the template for and the timing of the reporting of suspicious orders and transactions as well as other other aspects of the functioning of distributed ledger technology.

(6) Persons that are professionally engaged in arranging or executing transactions in crypto-assets should be able to delegate the prevention, monitoring, detection and identification of suspicious orders, transactions and other aspects of the functioning of distributed ledger technology within a group or to delegate the data analysis and the generation of alerts, subject to appropriate conditions. Such delegation should make it possible to share resources, to centrally develop and maintain monitoring systems and to build expertise in the context of monitoring orders and transactions. Such delegation should not prevent the competent authorities from assessing, at any time, whether the systems, arrangements and procedures of the person to whom the functions are delegated are effective to comply with the obligation to prevent, monitor and detect market abuse. The obligation to report as well as the responsibility to comply with this Regulation and with Article 92 of Regulation (EU) No 2023/1114 should remain with the delegating person.

(7) Crypto asset service providers operating a trading platform should have appropriate trading rules contributing to the prevention of market abuse. These entities should also have facilities to replay the order book in order to analyse the trading activity.

(8) A single and harmonised template for electronically submitting a STOR should assist compliance with the requirements set out in this Regulation and in Article 92 of Regulation (EU) No 2023/1114 in markets where orders and transactions are inherently cross-border. It should also facilitate the efficient sharing of information on suspicious orders and transactions between competent authorities in cross-border investigations.

(9) The relevant information fields contained in the STOR template, if completed clearly, comprehensively, objectively and accurately, should assist the competent authorities to promptly assess the suspicion and initiate relevant actions. The STOR template should therefore allow the persons submitting the STOR report to provide the information considered relevant about the suspicious orders, transactions or other aspects of the functioning of the distributed ledger technology reported and to explain the reasons for the suspicion. The STOR template should also allow to provide personal data that would make it possible to identify the persons involved in the suspicious activity and assist the competent authorities in the conduct of investigations. Such information should be provided at the outset, so that the integrity of the investigation is not compromised by the potential necessity for a competent authority to revert in the course of an investigation to the person who submitted the STOR.

(10) To facilitate the submission of a STOR, the template should allow for the attachment of documents and materials considered necessary to support the notification made, including in the form of an annex listing the orders or transactions relevant for the same report and detailling their prices and volumes. In addition, the template should also allow for the reporting of suspicious behaviours connected to the functioning of the distributed ledger technology.

(11) Persons professionally arranging or executing transactions in crypto-assets should not notify all orders received or transactions conducted that have triggered an internal alert. Such a requirement would be inconsistent with the requirement to assess on a case-by-case basis whether there are reasonable grounds for suspicion.

(12) The analysis of orders, transactions or other aspects of the functioning of the distributed ledger technology should factor in not only the internal information of the person professionally arranging or executing transactions in crypto-assets, but all the information publicly available, such as the information regarding transactions embedded in a public ledger system.

(13) The STORs should be submitted to the relevant competent authority without delay once a reasonable suspicion about the existence of market abuse has been formed. The analysis as to whether or not a given order or transaction is to be considered suspicious should be based on facts, not speculation or presumption and should be carried out as quickly as practicable. Delaying the submission of a report in order to incorporate further suspicious orders, transactions or other aspects of the functioning of the distributed ledger technology or accumulating several STORs are irreconcilable with the obligation to act without delay, where a reasonable suspicion has already been formed. In any case the submission of a STOR should be assessed on a case-by-case

basis to determine if several orders, transactions or other aspects of the functioning of the distributed ledger technology could be reported in a single STOR.

(14) There might be circumstances when a reasonable suspicion of market abuse is formed some time after the suspected activity occurred, due to subsequent events or available information. This should not be a reason for not reporting the suspected activity to the competent authority. In order to demonstrate compliance with the reporting requirements in those specific circumstances, the person submitting the report should be able to justify the time discrepancy between the occurrence of the suspected activity and the formation of the reasonable suspicion of market abuse having been committed, being committed or likely to be committed.

(15) The ability to recall and review the analysis performed on STORs which have been submitted, as well as those suspicious orders, transactions and behaviours connected to the functioning of the distributed ledger technology which were analysed, but in relation to which it was concluded that the grounds for suspicion were not reasonable, will assist persons professionally executing or arranging transactions in crypto-assets in exercising their judgement when considering subsequent suspicious orders or transactions.

(16) The analysis performed on suspicious orders, transactions, behaviours and other aspects connected to the functioning of the distributed ledger technology which did not lead to a STOR assists those persons in refining their surveillance systems and in detecting patterns of repeated behaviour, the aggregate of which could, considered as a whole, result in a reasonable suspicion of market abuse. Furthermore, the above records will also assist in evidencing compliance with the requirements laid down in this Regulation and facilitate the performance by competent authorities of their supervisory, investigatory and enforcement functions under Regulation (EU) No 2023/1114.

(17) Considering that markets in crypto-assets are inherently cross-border, it is necessary to specify coordination procedures between the relevant competent authorities for the detection and sanctioning of market abuse in case of cross-border market abuse situations. These coordination procedures should ensure that there are no conflicting investigations or enforcement activities. In this context, cross border market abuse situations should include at least cases in which suspicious transactions are carried out in a Member State concerning a crypto-asset that is admitted to trading in another Member State and cases in which the relevant crypto-asset service provider is operating in more than one Member State.

(18) It is also necessary to lay down provisions for the transmission of STORs on crypto-assets among competent authorities. Such requirements are critical, in the absence of a transaction reporting regime, to ensure efficient market supervision and enforcement while preventing the transmission of a massive flow of information that would not be useful for the receiving authority.

(19) Any processing of personal data under this Regulation should be carried out in compliance with Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. The data minimisation principle should be complied with where personal data are collected to ensure compliance with this Regulation.

(20) This Regulation is based on the draft regulatory technical standards submitted by the European Securities and Markets Authority to the Commission ('ESMA').

(21) ESMA has conducted open public consultations on the draft regulatory technical standards on which this Regulation is based, analysed the potential related costs and benefits and requested the advice of the Securities Markets Stakeholder Group established in accordance with Article 37 of Regulation (EU) No 1095/2010 of the European Parliament and the Council[17],

HAS ADOPTED THIS REGULATION:

Article 1

Definitions

For the purposes of this Regulation, the following definitions shall apply:

(a) 'suspicious transaction and order report' (STOR) means the report on suspicious orders or transactions, including any cancellation or modification thereof, and other aspects of functioning of the distributed ledger technology where circumstances might exist indicating that market abuse has been committed, is being committed or is likely to be committed.

(b) 'electronic means' are means of electronic equipment for the processing (including digital compression), storage and transmission of data, employing wires, radio, optical technologies, or any other electromagnetic means;

(c) 'group' means a group as defined in Article 2(11) of Directive 2013/34/EU of the European Parliament and of the Council[18];

[17] Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC (OJ L 331, 15.12.2010, p. 84).
[18] Directive 2013/34/EU of the European Parliament and of the Council of 26 June 2013 on the annual financial statements, consolidated financial statements and related reports of certain types of undertakings, amending Directive 2006/43/EC of the European Parliament and of the Council and repealing Council Directives 78/660/EEC and 83/349/EEC (OJ L 182, 29.6.2013, p. 19).

(d) ‘order’ means each and every order, including each and every quote, irrespective of whether its purpose is initial submission, modification, update or cancellation of an order and irrespective of its type;

(e) ‘algorithmic trading’ means trading in crypto-assets where a computer algorithm automatically determines individual parameters of orders such as whether to initiate the order, the timing, price or quantity of the order or how to manage the order after its submission, with limited or no human intervention, and does not include any system that is only used for the purpose of routing orders to one or more trading platform or for the processing of orders involving no determination of any trading parameters or for the confirmation of orders or the post-trade processing of executed transactions;

(f) ‘cross-border market abuse situations’ mean at least situations in which:

(i) more than one competent authority is competent to detect, investigate or sanction a potential market abuse case; or

(ii) cooperation between two or more competent authorities is necessary to detect, investigate or sanction a potential market abuse case.

SECTION 1

APPROPRIATE ARRANGEMENTS, SYSTEMS AND PROCEDURES TO PREVENT, DETECT AND REPORT MARKET ABUSE, AND THE TEMPLATE TO BE USED BY PERSONS PROFESSIONALLY ARRANGING OR EXECUTING TRANSACTIONS

Article 2

General requirements

1. Persons professionally arranging or executing transactions in crypto-assets shall establish and maintain arrangements, systems and procedures that ensure:

(a) effective and ongoing monitoring, for the purposes of preventing, detecting and identifying orders and transactions where circumstances might exist indicating that market abuse has been committed, is being committed or is likely to be committed, of all orders received and transmitted, and all transactions in crypto-assets executed;

(b) effective and ongoing monitoring of aspects of the functioning of the distributed ledger technology, for the purposes of detecting and identifying other aspects of the functioning of the distributed ledger technology, such as the consensus mechanism, where circumstances might exist indicating that

market abuse has been committed, is being committed or is likely to be committed;

(c) the transmission of STORs to competent authorities in accordance with the requirements set out in this Regulation and using the template set out in the Annex.

2. The obligations referred to in paragraph 1 shall apply to orders, transactions and other aspects of the functioning of the distributed ledger technology which might constitute market abuse and shall apply irrespective of:

(a) the capacity in which the order is placed or the transaction is executed;

(b) the types of clients concerned;

(c) whether the orders were placed or transactions executed on or outside a trading platform.

3. Persons professionally arranging or executing transactions in crypto-assets shall ensure that the arrangements, systems and procedures referred to in paragraph 1:

(a) are appropriate and proportionate in relation to the scale, size and nature of their business activity;

(b) are regularly assessed, at least through an annually conducted audit and internal review, and updated when necessary;

(c) are clearly documented in writing, including any changes or updates to them, for the purposes of complying with this Regulation, and that the documented information is maintained for a period of five years.

4. Persons professionally arranging or executing transactions in crypto-assets shall, upon request, provide the competent authority with the information on the assessment referred to in paragraph 3, including information on the level of automation put in place.

Article 3

Prevention, monitoring and detection

1. Persons professionally arranging or executing transactions in crypto-assets shall, to a degree which is appropriate and proportionate in relation to the scale, size and nature of their business activity, employ ICT systems and have in place procedures which assist the prevention and detection of market abuse or attempted market abuse.

The systems and procedures referred to in the first subparagraph shall include ICT systems capable of deferred automated reading, replaying and analysis of order book data, and such systems shall have sufficient capacity to operate in an algorithmic trading environment.

2. The arrangements, systems and procedures referred to in Article 2(1) shall:

   (a) cover the full range of trading activities undertaken by the persons professionally arranging or executing transactions in crypto-assets;

   (b) produce alerts indicating activities requiring further analysis for the purposes of detecting potential market abuse;

   (c) allow crypto-asset service providers operating a trading platform for the analysis, individually and comparatively, of each and every transaction executed, and order placed, modified, cancelled, or rejected in the systems of the trading platform. In case of repeated behaviours observed on the same trading platform, the system of the crypto-asset service providers operating a trading platform shall also aim at preventing such behaviour from taking place again;

   (d) allow persons professionally arranging or executing transactions in crypto-assets for the analysis, individually and comparatively of each and every transaction executed and order placed, modified, cancelled or rejected inside and outside a trading platform. This requirement is applicable irrespective of whether or not the orders and transactions are placed and executed by means of the distributed ledger.

3. Persons professionally arranging or executing transactions in crypto-assets shall put in place and maintain arrangements and procedures that ensure an appropriate level of human analysis in the prevention, monitoring, detection and identification of transactions, orders and aspects of the functioning of the distributed ledger technology that indicate the likelihood or existence of market abuse behaviours.

4. A person professionally arranging or executing transactions in crypto-assets may outsource to a third party or to a legal person forming part of the same group (the 'provider'), by written agreement, the performance of functions relating to prevention, monitoring, detection and identification of orders, transactions or other aspects of the functioning distributed ledger technology that could constitute market abuse, including the performance of data analysis, including order and transaction data, and the generation of alerts. The person delegating those functions shall remain fully responsible for discharging all of its obligations under this Regulation and Article 92 of Regulation (EU) No 2023/1114 and, where the functions are delegated to a third party, shall comply at all times with the following conditions:

   (a) it shall retain the expertise and resources necessary for evaluating the quality of the services provided and the organisational adequacy of the providers,

for supervising the delegated services and for the management of the risks associated with the delegation of those functions on an ongoing basis;

(b) it shall have direct access to all the relevant information regarding the data analysis and the generation of alerts.

The written agreement shall contain the description of the rights and obligations of the person outsourcing the tasks referred to in the first subparagraph and those of the provider. It shall also set out the grounds that allow the person delegating the functions to terminate such agreement.

5. As part of the arrangements and procedures referred to in Article 2, persons professionally arranging or executing transactions in crypto-assets shall maintain the information documenting the analysis carried out with regard to orders, transactions and aspects of the functioning of distributed ledger technology that could constitute market abuse for a period of five years. That information shall include the analysis made and the reasons for submitting or not submitting a STOR. That information shall be provided to the competent authority upon request.

Article 4

Training

Persons professionally arranging or executing transactions in crypto-assets shall organise and provide effective and comprehensive training to the staff involved in the prevention, monitoring, detection and identification of orders, transactions and other aspects of the functioning of the distributed ledger technology that could indicate the existence of market abuse, including the staff involved in the processing of orders and transactions or in charge of the functioning of the distributed ledger technology. Such training shall take place on a regular basis and shall be appropriate and proportionate in relation to the scale, size and nature of the business.

Article 5

Reporting obligations

1. Persons professionally arranging or executing transactions in crypto-assets shall establish and maintain effective arrangements, systems and procedures that enable them to assess, for the purpose of submitting a STOR, whether with reference to an order, a transaction or other aspects of the distributed ledger technology there are circumstances indicating that market abuse has been committed, is being committed or is likely to be committed. Those arrangements, systems and procedures shall include an appropriate level of human analysis.

2. Persons professionally arranging or executing transactions in crypto-assets shall ensure that STORs are based on facts and analysis, considering all the information available to them.

3. Persons professionally arranging or executing transactions in crypto-assets shall ensure that the arrangements and procedures referred to in Article 2 guarantee and maintain the confidentiality of the information. In particular, these persons shall have in place procedures to ensure that the person in respect of which the STOR was submitted and anyone who is not required to know about the submission of a STOR by virtue of their function or position within the reporting person is not informed of:

    (a) the generation of alerts or the assessment that may lead to the submission of a STOR. This includes that the reporting person will complete the STOR without sending requests of information to the person in respect of which the STOR may be submitted to complete certain fields;

    (b) the submission or the intention to submit a STOR to the competent authority.

Article 6

Timing of STORs

1. Persons professionally arranging or executing transactions in crypto-assets shall ensure that they have in place effective arrangements, systems and procedures for the submission of a STOR without delay, in accordance with Article 92 of Regulation (EU) No 2023/1114, once reasonable suspicion of market abuse is formed.

2. The arrangements, systems and procedures referred to in paragraph 1 shall entail the possibility to report STORs in relation to transactions, orders or other aspects of the functioning of the distributed ledger technology which occurred in the past, where suspicion has arisen in the light of subsequent events or information. In such cases, the person professionally arranging or executing transactions in crypto-assets shall explain in the STOR to the competent authority the delay between the suspected breach and the submission of the STOR according to the specific circumstances of the case.

3. Persons professionally arranging or executing transactions in crypto-assets shall submit to the competent authority any relevant additional information which they become aware of after the STOR has been originally submitted, and shall provide any information or document requested by the competent authority.

Article 7

Content of STORs

1. Persons professionally arranging or executing transactions in crypto-assets shall submit a STOR using the template set out in the Annex.

2. The persons referred to in paragraph 1 submitting the STOR shall complete the information fields relevant to the reported orders, transactions or other aspects of functioning of the distributed ledger technology in a clear and accurate manner.

Article 8

Means of transmission

1. Persons professionally arranging or executing transactions in crypto-assets shall submit a STOR, including any supporting documents or attachments, to the competent authority referred to in Article 92(1) of Regulation (EU) No 2023/1114 using the electronic means specified by that competent authority.

2. Competent authorities shall publish on their website the electronic means referred to in paragraph 1. Those electronic means shall ensure that completeness, integrity and confidentiality of the information are maintained during the transmission.

SECTION 2

COORDINATION PROCEDURES BETWEEN COMPETENT AUTHORITIES FOR DETECTION AND SANCTIONING OF MARKET ABUSE

Article 9

Coordination procedures for the detection of cross-border market abuse situations

In case of cross-border market abuse situations, the competent authority who receives the STOR shall transmit it without undue delay to the other competent authorities concerned, including, where relevant, to the competent authorities of the trading platforms where the crypto-asset is admitted to trading or for which a request for admission to trading has been made.

Article 10

Procedure, timing and form for the exchange of STOR between competent authorities

1. Competent authorities shall transmit STORs by using the form of unsolicited information specified in Annex IV of Commission Implementing Regulation (EU) 2024/2545 with regard to standard forms, templates and procedures for the cooperation and exchange of information between competent authorities].

2. The transmitting competent authority shall attach the STOR to the form referred to in paragraph 1, without being required to translate it into the language of the receiving competent authority. The transmitting competent authority shall include any additional documents provided in the STOR, specifying the legal basis for the provision of the information.

Article 11

Coordination procedures for the detection and sanctioning of cross-border market abuse situations

In case of cross-border market abuse situations, the following provisions apply:

(a) where a competent authority suspects that cross-border market abuse has taken place, may have taken place or may be taking place, it shall report without undue delay the status of its preliminary assessment to the other competent authorities concerned including, where applicable, the competent authorities of the trading platforms where the crypto-asset is admitted to trading. When informed about cross-border market abuse situations, the receiving competent authorities shall share information about the planning or existence of any supervisory activity or measure or, where applicable and where such information is available to the competent authority, about an existing criminal investigation on the same case without undue delay;

(b) in presence of cross-border market abuse situations, the competent authorities concerned shall periodically update each other, inform each other of significant interim developments and coordinate their supervisory and enforcement actions;

(c) where a competent authority has formally initiated an investigation, enforcement activity or, where applicable, is aware of a criminal investigation, it shall inform the other competent authorities concerned including, where applicable, the competent authorities of the trading platforms where the crypto-asset is admitted to trading. The reporting competent authority may inform ESMA as well;

(d) where two or more competent authorities have initiated an investigation or enforcement activity, any of them may request the coordination of ESMA at any point in time.

Article 12

Entry into force

This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

For the Commission

The President

[For the Commission

On behalf of the President

[Position]

ANNEX

STOR template

*Please note that **all** fields in Sections 1-4 are mandatory. Where information cannot be provided for a specific field, please indicate "NA" and briefly explain the reasons thereof.*	
SECTION 1 — IDENTITY OF ENTITY/PERSON SUBMITTING THE STOR Persons professionally arranging or executing transactions in crypto assets — Specify in each case:	
Name of the natural person	[First name(s) and surname(s) of the natural person in charge of the submission of the STOR within the submitting entity.]
Position within the reporting entity	[Position of the natural person in charge of the submission of the STOR within the submitting entity.]
Name of the reporting entity	[Full name of the reporting entity, including for legal persons: — the legal form as provided for in the register of the country pursuant to the law of which it is incorporated, where applicable, and — the Legal Entity Identifier (LEI) code in accordance with ISO 17442 LEI code.]
Address of the reporting entity	[Full address (e.g. street, street number, postal code, city, state/province) and country.]
Acting capacity of entity with respect to the orders, transactions or behaviours related to the functioning of the distributed ledger technology that could constitute market abuse	[Description of the capacity in which the reporting entity was acting with regards to the order(s), transaction(s) or behaviour(s) related to the functioning of the distributed ledger technology that could indicate the existence of market abuse, e.g. executing orders on behalf of clients, operating a trading platform...]
Type of trading activity (market making, arbitrage etc.) and type of crypto-asset traded by the reporting entity	[Description of any corporate, contractual or organisational arrangements or circumstances or relationships.]

Contact for additional request for information	[Person to be contacted within the reporting entity for additional request for information relating to this report (e.g. compliance officer) and relevant contact details: — first name(s) and surname(s), — position of the contact person within the reporting entity, — professional e-mail address, — professional phone number.]
Have the facts already been reported to public authorities?	Please state whether the facts have already been reported to public authority (and in that case indicate the name of the authority).
SECTION 2 — TRANSACTION/ORDER/BEHAVIOUR AND OTHER ASPECTS RELATED TO THE FUNCTIONING OF THE DISTRIBUTED LEDGER TECHNOLOGY	
Description of the crypto-asset:	Describe the crypto-asset(s) which is the subject of the STOR, specifying: — the full name (including Digital Token Identifier (DTI) in accordance with ISO 24165-2 or an equivalent unique identifier as referred to in Article 15 of Commission Delegated Regulation (EU) XXXX/XX (RTS on record-keeping) specifying records to be kept of all crypto-asset services, activities, orders and transactions undertaken) or description of the crypto-asset in the absence of DTI. If the suspicious behaviour involves a trading pair, please list both crypto-assets in the pair, — the type of crypto-asset (asset-referenced token (ART), e-money token (EMT), other crypto-asset) and for ARTs and EMTs, the value, right or official currency (or combination thereof) which the crypto-asset references in order to maintain a stable value.
Name(s) of the distributed ledger(s):	[Provide the full name(s) of the distributed ledger(s) where the suspicious behaviour was observed]
Trading platform where order was placed or the transaction was executed	[Specify name and Market Identifier Code (MIC) in accordance with ISO 10383 to identify the trading platform where the order was placed or the transaction was executed.

	If the order/transaction was not identified in a trading platform, please mention 'outside a trading platform' and the LEI of the CASP(s) that carried out the transaction if applicable.]
Location (country)	[Full name of the country and the ISO 3166-1 two-character country code.] [Specify: — where the order is given — where the order is executed, — where the behaviour related to functioning of the distributed ledger technology takes place.]
Description of the order, transaction or suspicious behaviour related to the functioning of the distributed ledger technology	[Describe at least the following characteristics of the order(s) transaction(s) or behaviour(s) reported — date(s) and time(s) of the order(s), transaction(s) or behaviour(s). (Dates and times should be reported in UTC per the format in ISO 8601). — transaction reference number or order reference number or transaction hash. — settlement date and time, — purchase price/sale price, — volume/quantity of crypto-assets, — for orders only, the type of order (e.g. 'buy with limit EUR x'), [Where there are multiple orders or transactions that could constitute market abuse the details on the prices and volumes of such orders and transactions can be provided to the competent authority in an Annex to the STOR.] — Information on the order cancellation or alteration including: — the nature of the alteration (e.g. change in price or quantity) and the extent of the alteration,

	[Where there are multiple orders or transactions that could constitute insider dealing, market manipulation or attempted insider dealing or market manipulation, the details on the prices and volumes of such orders and transactions can be provided to the competent authority in an Annex to the STOR.] — the means to alter the order (e.g. via e-mail, phone, etc.). In case of reporting a suspicious behaviour related to the functioning of the distributed ledger, please provide as much detail as possible, including the impact it had on the validation of transactions and the method used to alter the functioning of the distributed ledger.
SECTION 3 — DESCRIPTION OF THE NATURE OF THE SUSPICION	
Nature of the suspicion	[Specify the type of breach the reported order(s), transaction(s), behaviour(s) related to the functioning of the distributed ledger functioning, could constitute market abuse].
Reasons for the suspicion	[Description of the activity (transactions and orders, way of placing the orders or executing the transaction and characteristics of the orders and transactions that make them suspicious, behaviours related to the functioning of the distributed ledger functioning) and how the matter came to the attention of the reporting person and specify the reasons for suspicion. For crypto-assets admitted to trading on/traded on a trading platform, a description of the nature of the order book interaction/transactions that could constitute market abuse.]
SECTION 4 — IDENTIFICATION OF PERSON(S) RESPONSIBLE FOR THE ORDERS, TRANSACTIONS OR BEHAVIOUR RELATED TO THE FUNCTIONING OF THE DISTRIBUTED LEDGER TECHNOLOGY THAT COULD CONSTITUTE MARKET ABUSE (‘SUSPECTED PERSON’)	
Name	[For natural persons: the first name(s) and the last name(s).] [For legal persons: full name including legal form as provided for in the register of the country pursuant to the

	laws of which it is incorporated, if applicable, and Legal Entity Identifier (LEI) code in accordance with ISO 17442.]
National Identification Number	[Number and/or text]. [If the National Identification Number is not applicable or known, provide a date of birth (for natural persons only) in the ISO 8601 format]
Address	[Full address (e.g. street, street number, postal code, city, state/province) and country.]
Information about the employment: — Place — Position	[Information about the employment of the suspected person, from information sources available internally to the reporting entity (e.g. account documentation in case of clients, staff information system in case of an employee of the reporting entity).]
Account number(s) and wallet address(es)	[Numbers of the cash account(s), any joint accounts or any Powers of Attorney on the account the suspected entity/person holds. Wallet address(es) involved in the transaction or suspected behaviour]
Client identifier	[In case the suspected person is a client of the reporting entity.]
Relationship with the issuer of the crypto-asset concerned	[Description of any corporate, contractual or organisational arrangements or circumstances or relationships]
SECTION 5 — ADDITIONAL INFORMATION Background or any other information considered by the reporting entity relevant to the report	
[The following list is indicative and not exhaustive. Other information deemed useful by the reporting person may be provided where relevant to the STOR.] — The position of the suspected person (e.g. retail client, institutions), — The nature of the suspected entity's/person's intervention (on own account, on behalf of a client, validator of transactions in a distributed ledger system, other).	

— Where the suspected behaviour is conducted on a DLT, other relevant information may include:

— whether the transaction passed through a public or private (encrypted) queue of transactions (i.e. mempool) before it was validated on the DLT;

— whether the DLT is public (permissionless) or private (permissioned);

— potential interactions with smart contracts, for instance specification of the contract address and the function called;

— The size of the suspected entity's/person's portfolio,

— The date on which the business relationship with the client started if the suspected entity/person is a client of the reporting person/entity,

— The type of activity of the trading desk, if available, of the suspected entity,

— Trading patterns of the suspected entity/person. For guidance, the following are examples of information that may be useful:

— trading habits of the suspected entity/person,

— comparability of the size of the reported order/transaction with the average size of the orders submitted/transactions carried out by the suspected entity/person for the past 12 months,

— habits of the suspected entity/person in terms of crypto-assets it has traded for the past 12 months, in particular whether the reported order/transaction relates to a crypto-asset which has been traded by the suspected entity/person for the past year.

— Other entities/persons known to be involved in the orders or transactions of which could constitute market abuse:

— Names,

— Activity (e.g. executing orders on behalf of clients, dealing on own account, operating a trading platform, validating transactions.)]

SECTION 6 — DOCUMENTATION ATTACHED

[List the supporting attachments and material together provided with this STOR].

Examples of such documentation are e-mails, recordings of conversations, order/transaction records, distributed ledger technology records, confirmations, broker reports, Powers of Attorney documents, and comment by media where relevant.

Where the detailed information about the orders/transactions/behaviours related to the functioning of the distributed ledger technology referred to in Section 2 of this template is provided in a separate annex, indicate the title of that annex.]