Official Journal
of the European Union

EN
L series

2025/885

20.8.2025

COMMISSION DELEGATED REGULATION (EU) 2025/885

of 29 April 2025

supplementing Regulation (EU) 2023/1114 of the European Parliament and of the Council with regard to regulatory technical standards specifying the arrangements, systems and procedures to prevent, detect and report market abuse, the templates to be used for reporting suspected market abuse, and the coordination procedures between the 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 ([1]), and in particular Article 92(2), third subparagraph, thereof,

Whereas:

(1) Requirements for the arrangements, procedures and systems that persons professionally arranging or executing transactions in crypto-assets are to have in place for the reporting of orders, transactions and other aspects of the functioning of distributed ledger technology (DLT), including the consensus mechanism, where there might exist circumstances indicating that market abuse has been committed, is being committed or is likely to be committed are necessary. Such requirements are critical and should assist in the prevention and detection of market abuse. Those requirements should also assist in ensuring that 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) 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 DLT, in accordance with the scale, size and nature of the business activity of the person professionally arranging or executing transactions. Such systems should provide for human analysis carried out by appropriately trained staff based on objective information at the disposal of the reporting entity. The entity should collect additional personal data, only to ensure appropriate human analysis. To allow for further analysis of potential insider dealing or market manipulation or attempted insider dealing or market manipulation, the systems for monitoring market abuse should be capable of producing alerts in line with specified parameters. The access to such alerts should be recorded to ensure that they are only used for detecting market abuse. The whole process is likely to require some level of automation.

(3) To analyse whether the arrangements, systems and procedures to prevent and detect market abuse are appropriate, it is necessary to assess the impact that the person that professionally arranges or executes transactions may have on the market. As part of that assessment, such persons should assess whether they have a significant or dominant position in any crypto-asset market asset segment in which case those arrangements, systems and procedures should be proportionate to their position.

(4) The prevention and detection of market abuse requires an ongoing monitoring of all orders and transactions arranged or executed by persons that professionally arrange or execute transactions, irrespective of whether those orders and transactions are executed on the distributed ledger ('on-chain') or outside the distributed ledger ('off-chain'), including transfers of crypto assets to or from accounts of clients of the same crypto-asset service provider.

([1]) OJ L 150, 9.6.2023, p. 40, ELI: http://data.europa.eu/eli/reg/2023/1114/oj.

(5) To facilitate and promote a consistent approach and practices across the Union in relation to the prevention, detection and sanctioning of market abuse, it is necessary to lay down detailed provisions harmonising the content of, the template for and the timing of the reporting of suspicious orders and transactions and other aspects of the functioning of DLT.

(6) To share resources, to centrally develop and maintain monitoring systems, and to build expertise in the context of monitoring suspicious orders and transactions, persons that professionally arrange or execute transactions in crypto-assets should be able to delegate the prevention and detection of such orders, transactions and other aspects of the functioning of DLT within a group, or to delegate the data analysis and the generation of alerts, subject to appropriate conditions. Such delegation should neither prevent the competent authorities from assessing at any time, whether the arrangements, systems and procedures of the person to whom the functions are delegated are effectively in line with the obligation to prevent and detect market abuse. The obligation to report and the responsibility to comply with this Regulation and with Article 92 of Regulation (EU) 2023/1114 should remain with the delegating person.

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

A single and harmonised template for electronically submitting a suspicious transaction and order report ('STOR') should facilitate the efficient sharing of information on suspicious orders and transactions between competent authorities in cross-border investigations.

(8) The information fields in such a STOR template, where completed clearly, comprehensively, objectively and accurately, should assist the competent authorities to promptly assess such suspicious orders and transactions and take the necessary action. Such STOR template should therefore enable the persons submitting the STOR to provide the information that competent authorities consider relevant about 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 enable the persons submitting the STOR to provide personal data that would make it possible to identify the persons involved in the suspicious activity and assist the competent authorities in their 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 during an investigation to the person who submitted the STOR. Any processing of personal data under this Regulation should be carried out in compliance with Regulation (EU) 2016/679 of the European Parliament and of the Council ([2]) 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 in particular should be complied with where personal data are collected to ensure compliance with this Regulation.

(9) To facilitate the submission of a STOR, the template should allow for the attachment of documents and materials that are necessary to support the notification made, including in the form of an annex that lists the suspicious orders or transactions and detailing their prices and volumes. In addition, the STOR template should allow for the reporting of suspicious behaviours connected to the functioning of the DLT.

(10) 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.

(11) The analysis of orders, transactions or other aspects of the functioning of the DLT 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, including information about transactions embedded in a public ledger system.

([2]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

(12) The STORs should be submitted to the competent authority without delay once a reasonable suspicion about the existence of market abuse has been formed. The analysis as to whether 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 practicably possible. Delaying the submission of a report to incorporate further suspicious orders, transactions or other aspects of the functioning of the DLT or accumulating several STORs would be irreconcilable with the obligation to act without delay, where a reasonable suspicion has already been formed. In any case, persons professionally arranging or executing transactions in crypto-assets should assess on a case-by-case basis whether several orders, transactions or other aspects of the functioning of the DLT could be reported in a single STOR.

(13) There might be circumstances where a reasonable suspicion of market abuse is formed after the suspected activity occurred, due to subsequent events or available information. That should not be a reason for not reporting the suspected activity to the competent authority. To demonstrate compliance with the reporting requirements in those specific circumstances, the person submitting the STOR 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.

(14) To assist persons professionally arranging or executing transactions in crypto-assets in exercising their judgement when considering subsequent suspicious orders or transactions, they should be able to recall and review the analysis of STORs which have been submitted, and of those suspicious orders, transactions and behaviours connected to the functioning of the DLT which were analysed, but in relation to which the competent authority concerned concluded that the grounds for suspicion were not reasonable.

(15) To prevent market abuse to the maximum extent possible, persons professionally arranging or executing transactions in crypto-assets should be able to refine their surveillance systems and to detect patterns of repeated behaviour, the aggregate of which could, considered as a whole, result in a reasonable suspicion of market abuse. Those persons should therefore be required to analyse suspicious orders, transactions, behaviours and other aspects connected to the functioning of the distributed ledger technology which did not lead to a STOR and record such analyses. Such records should also assist such persons in evidencing compliance with Article 92 of Regulation (EU) 2023/1114 and should facilitate the performance by competent authorities of their supervisory, investigatory and enforcement functions under Article 92 of Regulation (EU) 2023/1114.

(16) Considering that markets in crypto-assets are inherently cross-border, it is necessary to specify coordination procedures between the competent authorities for the detection and sanctioning of market abuse in case of cross-border market abuse situations. Such coordination procedures should ensure that there are no conflicting investigations or enforcement activities. In that context, cross-border market abuse situations should include 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 crypto-asset service provider concerned is operating in more than one Member State.

(17) It is necessary to lay down provisions for the transmission of STORs 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.

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

(19) 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 and Markets Stakeholder Group established in accordance with Article 37 of Regulation (EU) No 1095/2010 of the European Parliament and the Council ([3]),

([3]) 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, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

(20) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 ([4]) and delivered their opinion on 22 January 2025,

HAS ADOPTED THIS REGULATION:

Article 1

Definitions

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

(1) '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 DLT where circumstances might exist indicating that market abuse has been committed, is being committed or is likely to be committed.

(2) '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;

(3) 'group' means a group as defined in Article 2, point (11), of Directive 2013/34/EU of the European Parliament and of the Council ([5]);

(4) '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.

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 DLT, for the purposes of detecting and identifying other aspects of the functioning of the distributed ledger technology, including 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.

([4]) Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([5]) 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, ELI: http://data.europa.eu/eli/dir/2013/34/oj).

2. The obligations referred to in paragraph 1 shall apply to orders, transactions and other aspects of the functioning of the DLT 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 are:

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

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

(c) clearly documented in writing, including any changes or updates to them, for the purposes of compliance with this Regulation, and that the documented information is maintained for a period of 5 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. The arrangements, systems and procedures referred to in Article 92(1) of Regulation (EU) 2023/1114 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 to detect potential market abuse;

(c) enable crypto-asset service providers operating a trading platform to:

(i) analyse, individually and comparatively, each transaction executed, and each order placed, modified, cancelled, or rejected in the systems of the trading platform;

(ii) prevent the occurrence of repeated behaviours observed on the same trading platform;

(d) enable persons professionally arranging or executing transactions in crypto-assets to analyse, individually and comparatively each transaction executed and each order placed, modified, cancelled or rejected inside and outside a trading platform, irrespective of whether or not the orders and transactions are placed and executed by means of the distributed ledger, and aspects of the functioning of DLT that could constitute market abuse.

2. 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. Persons professionally arranging or executing transaction in crypto-assets shall collect additional personal data, only for the sole purpose of ensuring appropriate level of human analysis.

3. For the purposes of Article 92(1) of Regulation (EU) 2023/1114, persons professionally arranging or executing transactions in crypto-assets shall, to a degree which is appropriate for, and proportionate in relation to, the scale, size, and nature of their business activity, employ ICT systems.

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

For the purposes of the second subparagraph, algorithmic trading means trading in crypto-assets where a computer algorithm automatically determines individual parameters of orders, including as to 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.

4. Persons professionally arranging or executing transactions in crypto-assets may by written agreement outsource to a third party or delegate to a legal person forming part of the same group, as defined in Article 2, point (11), of Directive 2013/34/EU of the European Parliament and of the Council [6] ('providers'), the functions relating to the prevention, monitoring, detection and identification of orders, transactions or other aspects of the functioning DLT that could constitute market abuse, including analysis of data, including order and transaction data, and the generation of alerts. Persons delegating or outsourcing those functions shall remain fully responsible for complying with all of their obligations under this Regulation and Article 92 of Regulation (EU) 2023/1114. Where those functions are outsourced to a third party, persons outsourcing those functions shall comply with the following requirements at all times:

(a) retain the expertise and resources necessary to:

  (i) evaluate the quality of the services provided and the organisational adequacy of the providers;

  (ii) supervise the outsourced services;

  (iii) manage of the risks associated with the outsourcing of those functions on an ongoing basis;

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

The written agreement referred to in the first subparagraph shall describe the rights and obligations of the person delegating or outsourcing the functions and those of the provider. It shall also set out the grounds on the basis of which the person delegating or outsourcing the functions can terminate that agreement.

5. As part of the arrangements, systems and procedures referred to in the first and second subparagraphs, 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 DLT that could constitute market abuse for a period of 5 years. That information shall include the analysis made and the reasons for submitting or not submitting a STOR. Persons professionally arranging or executing transactions in crypto-assets shall provide that information to the competent authority upon request.

[6] 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, ELI: http://data.europa.eu/eli/dir/2013/34/oj).

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 DLT 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 DLT. Such training shall take place on a regular basis and shall be appropriate and proportionate to the scale, size and nature of the business.

Article 5

Reporting of suspicious orders or transactions

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 DLT there might be 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 report a STOR:

(a) by using the STOR template set out in the Annex and completing the information fields relevant to the reported orders, transactions or other aspects of functioning of the DLT in a clear and accurate manner, including any supporting documents or attachments;

(b) using the electronic means specified by that competent authority.

For the purposes of point (b) of the first subparagraph, the competent authority shall specify on its website the electronic means to be used, and shall ensure that those electronic means ensure that the completeness, integrity, and confidentiality of the information are maintained during the transmission.

The STOR referred to in the first subparagraph shall be based on facts and analysis, considering all the information available to the persons professionally arranging or executing transactions in crypto-assets.

3. Persons professionally arranging or executing transactions in crypto-assets shall ensure and maintain the confidentiality of the information laid down in the report on suspicious orders or transactions and 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 the alerts referred to in Article 3(1), point (b);

(b) the assessment that may lead to the submission of a STOR;

(c) the fact 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;

(d) the submission of a STOR to the competent authority, or the intention to submit one.

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, 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 DLT which occurred in the past, where suspicion has arisen in the light of subsequent events or information. In such cases, persons professionally arranging or executing transactions in crypto-assets shall explain in the STOR 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 submitted, and shall provide any information or document requested by the competent authority.

Article 7

Exchange of reports between competent authorities

1. Competent authorities shall transmit STORs by using the form of unsolicited provision of information set out in Annex IV to Commission Implementing Regulation (EU) 2024/2545 ([7]).

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 8

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

1. A competent authority that suspects that cross-border market abuse has taken place, may have taken place, or may be taking place, shall report the status of its preliminary assessment to the other competent authorities concerned without undue delay, including, where applicable, to 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, without undue delay, share information about the planning or existence of any supervisory activity or measure or, where applicable and where such information is available to the receiving competent authority, about an existing criminal investigation on the same case.

2. Competent authorities concerned shall:

(a) periodically update each other about cross-border market abuse situations;

(b) inform each other about significant interim developments related to cross-border market abuse situations;

(c) coordinate their supervisory and enforcement actions.

([7]) Commission Implementing Regulation (EU) 2024/2545 of 24 September 2024 laying down implementing technical standards for the application of Regulation (EU) 2023/1114 of the European Parliament and of the Council with regard to standard forms, templates and procedures for the cooperation and exchange of information between competent authorities (OJ L, 2024/2545, 26.11.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2545/oj).

3. A competent authority that has formally initiated an investigation, enforcement activity or, where applicable, that is aware of a criminal investigation, shall inform the other competent authorities concerned thereof, 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.

4. Competent authorities having initiated or involved in an investigation or enforcement activity in the context of cross-border situations may request the coordination of ESMA.

5. For the purposes of this Article, 'cross-border market abuse situations' shall mean any of the following situations:

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

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

Article 9

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, 29 April 2025.

For the Commission
The President
Ursula VON DER LEYEN

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 DLT 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, if not the same as person in charge of the submitting of the STOR: — first name(s) and surname(s), — position of the contact person within the reporting entity, — professional email 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) 2025/1140 ([1]) 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. Where 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. Where the order/transaction was not identified in a trading platform, please mention 'outside a trading platform' and the LEI of the crypto-asset service provider that carried out the transaction where applicable.]
Location (country)	[Full name of the country and the ISO 3166-1 two-character country code.] [Specify where: — the order is given — the transaction is executed, — 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 DLT	[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 email, 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 DLT.

SECTION 3 – DESCRIPTION OF THE NATURE OF THE SUSPICION

Nature of the suspicion	[Specify the type of breach based on which the reported order(s), transaction(s), behaviour(s) related to the functioning of the DLT, 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 DLT) 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, where applicable, and Legal Entity Identifier (LEI) code in accordance with ISO 17442.]
National Identification Number	[Number and/or text]. [Where 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

Other information relevant to the report, depending on the activity

[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, including 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, where 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 is provided in a separate annex, indicate the title of that annex.]

([1]) Commission Delegated Regulation (EU) 2025/1140 of 27 February 2025 supplementing Regulation (EU) 2023/1114 of the European Parliament and of the Council with regard to regulatory technical standards specifying records to be kept of all crypto-asset services, activities, orders and transactions undertaken (OJ L, 2025/1140, 10.6.2025, ELI: http://data.europa.eu/eli/reg_del/2025/1140/oj).