

CRYPTOASSETS (MARKET ABUSE) INSTRUMENT 2026**Powers exercised**

- A. The Financial Conduct Authority (“the FCA”) makes this instrument in the exercise of the powers and related provisions in or under:
- (1) the following sections of the Financial Services and Markets Act 2000 (“the Act”):
 - (a) section 71N (Designated activities: rules);
 - (b) section 137T (General supplementary powers); and
 - (c) section 139A (Power of the FCA to give guidance);
 - (2) the following provisions of the Financial Services and Markets Act 2000 (Cryptoassets) Regulations 2026 (SI 2026/102):
 - (a) regulation 21 (Designated activity rules: market abuse in qualifying cryptoassets and related instruments);
 - (b) regulation 23 (Exclusions: insider dealing);
 - (c) regulation 26 (Public disclosure of inside information);
 - (d) regulation 27 (Public disclosure of inside information: delayed disclosure);
 - (e) regulation 30 (Systems and procedures for trading relevant qualifying cryptoassets and related instruments);
 - (f) regulation 31 (Insider lists for relevant qualifying cryptoassets and related instruments);
 - (g) regulation 32 (Cases in which sharing of information authorised or required); and
 - (h) regulation 34 (Legitimate cryptoasset market practice); and
 - (3) the other rule and guidance making powers listed in Schedule 4 (Powers exercised) to the General Provisions of the FCA’s Handbook.
- B. The rule-making powers listed above are specified for the purpose of section 138G(2) (Rule-making instruments) of the Act.

Commencement

- C. This instrument is one of a series of instruments which introduce or amend provisions of the Handbook relating to cryptoassets. These instruments all come into force on 25 October 2027, immediately after one another, in the following order:
- (1) Glossary (Cryptoassets) Instrument 2026;
 - (2) Cryptoassets (Stablecoins) Instrument 2026;
 - (3) Cryptoassets (Admission of Qualifying Cryptoassets to Trading and Offers of Qualifying Cryptoassets to the Public) Instrument 2026;
 - (4) Cryptoassets (Market Abuse) Instrument 2026;
 - (5) Cryptoassets (Intermediaries) Instrument 2026;

- (6) Cryptoassets (Trading Platforms, Transparency and Records) Instrument 2026;
- (7) Cryptoassets (Lending, Borrowing and Staking) Instrument 2026;
- (8) Cryptoassets (Safeguarding) Instrument 2026;
- (9) Cryptoassets (Client Assets Consequential) Instrument 2026;
- (10) Cryptoassets (Conduct and Firm Standards) Instrument 2026; and
- (11) Cryptoassets (COREPRU and CRYPTOPRU) Instrument 2026.

Amendments to the Handbook

- D. The Cryptoassets sourcebook (CRYPTO) is amended in accordance with the Annex to this instrument.

Citation

- E. This instrument may be cited as the Cryptoassets (Market Abuse) Instrument 2026.

By order of the Board
25 June 2026

Annex

Amendments to the Cryptoassets sourcebook (CRYPTO)

In this Annex, all text is new and is not underlined. Insert the following new chapter, CRYPTO 4, after CRYPTO 3 (Admission of qualifying cryptoassets to trading on a UK QCATP and offers to the public of qualifying cryptoassets admitted to trading).

4 Cryptoasset market abuse

4.1 Purpose, application and interpretation

Purpose and application

- 4.1.1 G The purpose of *CRYPTO* 4.2 to *CRYPTO* 4.6 is to set out *guidance* on key concepts and prohibited behaviours that could constitute *cryptoasset market abuse*. Those sections apply as follows:
- (1) *CRYPTO* 4.2 applies to all *persons* seeking general *guidance* on certain concepts relevant to *cryptoasset market abuse*;
 - (2) *CRYPTO* 4.3 applies to all *persons* seeking general *guidance* on *cryptoasset inside information*;
 - (3) *CRYPTO* 4.4 applies to all *persons* seeking general *guidance* on *cryptoasset insider dealing*;
 - (4) *CRYPTO* 4.5 applies to all *persons* seeking general *guidance* on *cryptoasset unlawful disclosure*; and
 - (5) *CRYPTO* 4.6 applies to all *persons* seeking general *guidance* on the factors and indicators to take into account in relation to behaviours that could constitute *cryptoasset market manipulation*.
- 4.1.2 G The purpose of *CRYPTO* 4.7 to *CRYPTO* 4.9 is to set out regulatory requirements and *guidance* that apply to *UK QCATP operators* and *cryptoasset intermediaries* in relation to the prevention, detection and disruption of *cryptoasset market abuse*. Those sections apply as follows:
- (1) In relation to insider dealing and market manipulation:
 - (a) *CRYPTO* 4.7 applies to *UK QCATP operators* in relation to establishing and maintaining effective systems and controls, as well as receiving notifications of suspicious orders from *cryptoasset intermediaries*; and
 - (b) *CRYPTO* 4.8 applies to *cryptoasset intermediaries* in relation to establishing and maintaining effective systems and controls, as well as transmitting notifications of suspicious orders to *UK QCATP operators*.

- (2) *CRYPTO 4.9 applies to large CATP operators in relation to the disclosure of information to other large CATP operators for the purposes of preventing, detecting and disrupting cryptoasset market abuse.*
- 4.1.3 G The purpose of *CRYPTO 4.10* is to set out requirements on, and give *guidance* to, *relevant issuers, persons responsible for the offer* and *UK QCATP operators* when publicly disclosing *cryptoasset inside information* and to ensure prompt disclosure of that information.
- 4.1.4 G The purpose of *CRYPTO 4.11* is to specify activities that are *legitimate cryptoasset market practices* in accordance with regulation 34 of the *Cryptoassets Regulations* and to set out the operational requirements for their implementation.
- 4.1.5 G The purpose of *CRYPTO 4.12* is to set out requirements on *relevant issuers, persons responsible for the offer* and *UK QCATP operators* in relation to drawing up, maintaining and updating *cryptoasset insider lists*.
- 4.1.6 G The purpose of *CRYPTO 4.13* is to draw attention to section 138A of the *Act*, which provides the *FCA* with the power to waive or modify the application of *FCA rules*.
- 4.1.7 G The scope of investments to which the *Cryptoassets Regulations* apply differs from that of the *Market Abuse Regulation*. The following should therefore be considered when applying these different legal frameworks to the different types of *cryptoasset*:
- (1) Whereas the *Market Abuse Regulation* applies, in particular, to *financial instruments* within the scope of article 2 of the *Market Abuse Regulation*, *cryptoasset market abuse* applies to *relevant qualifying cryptoassets and related instruments*, neither of which can be *financial instruments*.
 - (2) Whereas a *cryptoasset derivative* which is a *financial instrument* is one to which the *Market Abuse Regulation* may apply, a spot transaction involving a *cryptoasset* is one to which the *Cryptoassets Regulations* apply, where it comprises a *relevant qualifying cryptoasset* or *related instrument*.
 - (3) A *person* trading in *cryptoasset derivatives* and spot transactions in *cryptoassets* will need therefore to consider the *Market Abuse Regulation*, *MAR 1* and *CRYPTO 4*.
- 4.1.8 The *FCA's* statement of policy about the imposition, duration and amount of penalties in cases of *cryptoasset market abuse* required by section 124 of the *Act* is in *DEPP 6*.

Interpretation

- 4.1.9 G The following considerations may assist in the interpretation of this chapter:

- (1) *CRYPTO* 4.2 to *CRYPTO* 4.6 do not exhaustively describe all types of behaviour that may indicate *cryptoasset market abuse*. In particular, the descriptions of behaviour should be read in the light of:
 - (a) regulations 19, 22 and 24 of the *Cryptoassets Regulations* as making up the relevant type of *cryptoasset market abuse*; and
 - (b) any relevant descriptions of behaviour specified under regulations 23, 25 and 29 of the *Cryptoassets Regulations* which do not amount to *cryptoasset market abuse*.
- (2) *CRYPTO* 4.2 to *CRYPTO* 4.6 do not exhaustively describe all the factors to be taken into account in determining whether behaviour amounts to *cryptoasset market abuse*. The absence of a factor mentioned does not, of itself, amount to a contrary indication.
- (3) For the avoidance of doubt, any reference in *CRYPTO* 4 to ‘profit’ refers also to potential profits, avoidance of loss or potential avoidance of loss.
- (4) References are made in *CRYPTO* 4 to provisions in the *Cryptoassets Regulations*. The fact that other provisions of the *Cryptoassets Regulations* have not been referred to does not mean that they would not also assist readers or that they have a different status.

4.1.10 G Assistance in the interpretation of the *Handbook* (and, by extension, *CRYPTO* 4) is given in the Reader’s Guide, which can be found on the *FCA*’s website at <https://handbook.fca.org.uk/guides/reader-guide>, and in *GEN* 2 (Interpreting the Handbook). The Reader’s Guide includes an explanation of the status of the types of provision used.

4.2 Cryptoasset market abuse: general guidance

4.2.1 G Provisions in *CRYPTO* 4 are relevant to more than one of the types of behaviour which may amount to *cryptoasset market abuse*.

4.2.2 G *Cryptoasset market abuse* prevents full and proper market transparency, which is a prerequisite for trading for all economic actors in markets relating to *relevant qualifying cryptoassets* and *related instruments*.

4.2.3 G The *Cryptoassets Regulations* do not require the *person* engaging in the behaviour in question to have intended to commit *cryptoasset market abuse*.

4.2.4 G Where *persons* have taken all reasonable measures to prevent *cryptoasset market abuse* from occurring but nevertheless *persons* within their employment commit *cryptoasset market abuse* on their behalf, this should not be deemed to constitute *cryptoasset market abuse* by the *persons* taking all reasonable measures to prevent *cryptoasset market abuse* from occurring.

Acting jointly or in concert

- 4.2.5 G In accordance with regulation 39 of the *Cryptoassets Regulations*, a person contravenes a prohibition against *cryptoasset market abuse* whether the contravention is by that *person* alone or by that *person* jointly or in concert with one or more other *persons*.
- 4.2.6 G Examples of *persons* acting jointly or in concert could include, but are not limited to:
- (1) *cryptoasset intermediaries* who devise and recommend a trading strategy designed to result in *cryptoasset market abuse*;
 - (2) *persons* who encourage a *person* with *cryptoasset inside information* to disclose that information unlawfully; or
 - (3) *persons* who develop software in collaboration with a trader for the purpose of facilitating *cryptoasset market abuse*.

Factors that may be taken into account in relation to behaviour prior to a request for *admission to trading*, or to the *admission to trading* or to the commencement of trading

- 4.2.7 G (1) The factors in (2) may be taken into account in determining whether, and indicate that, a behaviour that takes place prior to:
- (a) a request for *admission to trading* of *qualifying cryptoassets*;
 - (b) the *admission to trading* of *qualifying cryptoassets*; or
 - (c) the commencement of trading of *qualifying cryptoassets*,
- contravenes the *Cryptoassets Regulations*.
- (2) The factors referred to in (1) are:
- (a) where a request for *admission to trading* of a *qualifying cryptoasset* on a UK *QCATP* is subsequently made; and
 - (b) whether the behaviour continues to have an effect once an application has been made for the *qualifying cryptoasset* to be *admitted for trading*, or once it has been *admitted to trading*, on a UK *QCATP*.

Cross-border cryptoasset market abuse

- 4.2.8 G Regulations 19(3) and 22(6) of the *Cryptoassets Regulations* provide that, for the purposes of the prohibitions against *cryptoasset market manipulation* and *cryptoasset insider dealing*, it is immaterial where the activities specified by regulations 19 and 22 of the *Cryptoassets Regulations* are carried out.

- 4.2.9 G (1) The *Cryptoassets Regulations* therefore recognise that *cryptoasset market abuse* may take place across cryptoasset markets as well as across borders. This can lead to significant market-wide risks.
- (2) The cross-border element of *cryptoassets* and their highly mobile nature means that *cryptoasset market abuse* can potentially occur on *overseas qualifying cryptoasset trading platforms*, including in a jurisdiction that does not impose equivalent cryptoasset regulation, and can directly or indirectly affect price formation on a *UK QCATP*.
- (3) The prohibitions and requirements therefore apply to actions and omissions concerning *relevant qualifying cryptoassets*, regardless of whether they take place in the *UK* or in another country or territory.

FCA rules

- 4.2.10 G There are no *rules* which permit or require a *person* to behave in a way that amounts to *cryptoasset market abuse*.

4.3 Cryptoasset inside information

- 4.3.1 G *Cryptoasset inside information* means, as defined in regulation 18(2) of the *Cryptoassets Regulations*, information of a precise nature, which has not been made public, relating, directly or indirectly, to:
- (1) a *relevant issuer* of a *relevant qualifying cryptoasset* or a *related instrument*;
 - (2) a *person responsible for the offer* of a *relevant qualifying cryptoasset* or a *related instrument*;
 - (3) an operator of a *UK QCATP* on which a *relevant qualifying cryptoasset* is:
 - (a) *admitted to trading*; or
 - (b) subject to an application seeking *admission to trading*; or
 - (4) a *relevant qualifying cryptoasset* or *related instrument*,
- which, if it were made public, would be likely to have a significant effect on the price of that *relevant qualifying cryptoasset* or *related instrument*.

Factors to be taken into account: made public

- 4.3.2 G The following factors may be taken into account in determining whether or not information has been made public, and are indications that it has (and therefore that it is not *cryptoasset inside information*):

- (1) whether the information has been disclosed on the website of a *relevant issuer, a person responsible for the offer* or a *UK QCATP operator*;
 - (2) whether the information is contained in records which are open to inspection by the public;
 - (3) whether the information is otherwise generally available, including through widely accessible social media platforms, or some other publication (including if it is only available on payment of a fee), or is derived from information which has been made public; and
 - (4) whether the information can be obtained by observation by members of the public without infringing rights or obligations of privacy, property or confidentiality.
- 4.3.3 G (1) In relation to the factors in *CRYPTO* 4.3.2G, it is not relevant that the information is only generally available outside the *UK*.
- (2) In relation to the factors in *CRYPTO* 4.3.2G(4), it is not relevant that the observation or analysis is only achievable by a *person* with above-average financial resources, expertise or competence.
- 4.3.4 G For example, if the holder of a *relevant qualifying cryptoasset* becomes aware of a large transfer involving another holder with a significant position in that cryptoasset (commonly referred to as a ‘whale alert’), or observes the transfer directly on a blockchain, the holder would be using information that has been made public to the extent the blockchain data concerned and whale alerts are publicly accessible.

Research and estimates

- 4.3.5 G (1) Research and estimates based on publicly available data should not be regarded as *cryptoasset inside information* and the mere fact that a transaction is carried out on the basis of research or estimates should not therefore be deemed to constitute use of *cryptoasset inside information*. However, for example, the information may constitute *cryptoasset inside information* where:
- (a) the publication or distribution of information is routinely expected by the market and where such publication or distribution contributes to the price-formation process of *relevant qualifying cryptoassets* or *related instruments*; or
 - (b) the information provides views from a recognised market commentator or institution which may inform the prices of *relevant qualifying cryptoassets* or *related instruments*.
- (2) Consideration must therefore be given to the extent to which the information is non-public and the possible effect on *relevant qualifying cryptoassets* or *related instruments* traded in advance of its publication

or distribution, to establish whether market actors would be trading on the basis of *cryptoasset inside information*.

Investor plans and strategies

- 4.3.6 G Information regarding an investor's own plans and strategies for trading should not be considered to be *cryptoasset inside information*, although information regarding a third party's plans and strategies for trading may amount to *cryptoasset inside information*.

Factors to take into account: pending orders

- 4.3.7 G Regulation 18(3) of the *Cryptoassets Regulations* provides that where any *person* to whom Chapter 2 of the *Cryptoassets Regulations* applies is executing orders for a *relevant qualifying cryptoasset* or a *related instrument* on behalf of clients, *cryptoasset inside information* also includes information of a precise nature, which has not been made public, conveyed by a client and relating both to the client's pending orders for a *relevant qualifying cryptoasset* or a *related instrument* and, directly or indirectly, to:

- (1) a *relevant issuer* of a *relevant qualifying cryptoasset* or a *related instrument*;
- (2) a *person responsible for the offer* of a *relevant qualifying cryptoasset* or a *related instrument*;
- (3) an operator of a *UK QCATP* on which a *relevant qualifying cryptoasset* is:
 - (a) *admitted to trading*; or
 - (b) subject to an application seeking *admission to trading*; or
- (4) a *relevant qualifying cryptoasset* or *related instrument*,

which, if it were made public, would be likely to have a significant effect on the price of that *relevant qualifying cryptoasset* or *related instrument*.

- 4.3.8 G In determining whether there is a pending order for a client in relation to regulation 18(3) of the *Cryptoassets Regulations*, a factor that may be taken into account is whether a *person* is approached by another in relation to a transaction, and:
- (1) the transaction is not immediately executed on an arm's length basis in response to a price quoted by that *person*; and
 - (2) the *person* concerned has taken on a legal or regulatory obligation relating to the manner or timing of the execution of the transaction.

Examples of cryptoasset inside information

- 4.3.9 G The following are examples of information that could amount to *cryptoasset inside information*, but are not intended to form an exhaustive list:
- (1) information relating to an *admission to trading*, or the cancellation of an *admission to trading*;
 - (2) information relating to the cancellation, refusal or withdrawal of a request for an *admission to trading*;
 - (3) information relating to a *qualifying stablecoin admitted to trading* on a *UK QCATP* or the issuer of such a stablecoin, which could affect its intended value or the issuer's ability to fulfil *redemption* requests, including disruption to payment channels or a significant restriction or interruption to *minting* or *redemption* processes;
 - (4) information on a code vulnerability that is known to a development team as a result of testing the code of the *relevant qualifying cryptoasset* prior to *admission to trading*;
 - (5) information held by a key governance body, or by an entity controlling a significant portion of the blockchain's validating infrastructure, regarding plans to introduce or reject a split in the blockchain's protocol (also known as a 'blockchain fork');
 - (6) information relating to significant changes in respect of a major cryptoasset market participant, such as mergers, acquisitions, changes to key personnel or joint ventures;
 - (7) information about a forthcoming distribution of free *relevant qualifying cryptoassets* (also known as an 'airdrop') or *burning*, potentially also including information about the magnitude, timing or cancellation of the 'airdrop' or the *burning*, and information about the selection or qualification mechanism to be used in respect of an airdrop; and
 - (8) information relating to changes to the arrangements of *market makers* and the addition or withdrawal of significant liquidity providers.

Ongoing processes

- 4.3.10 G Regulation 18(4)(a) to (c) of the *Cryptoassets Regulations* provides that:

- (1) information is to be considered of a precise nature if it indicates a set of circumstances which exists or which may reasonably be expected to come into existence, or an event which has occurred or which may reasonably be expected to occur, where it is specific enough to enable a conclusion to be drawn as to the possible effect of that set of circumstances or event on the price of a *relevant qualifying cryptoasset* or *related instrument*;

- (2) in the case of an ongoing process that is intended to bring about, or that results in, a particular circumstance or event, that future circumstance or event, and also the intermediate steps of that process which are connected with bringing about or resulting in that future circumstance or event, is to be considered precise information; and
- (3) an intermediate step in an ongoing process is to be considered *cryptoasset inside information* if, in and of itself, it satisfies the criteria of *cryptoasset inside information* referred to in regulation 18(4)(a) of the *Cryptoassets Regulations*.

4.3.11 G The following considerations may assist in determining when *cryptoasset inside information* could arise in an ongoing process:

- (1) Where *cryptoasset inside information* concerns a process which occurs in stages, each stage of the process, as well as the overall process, could constitute *cryptoasset inside information*.
- (2) An intermediate step in an ongoing process may itself constitute a set of circumstances or an event:
 - (a) which exists; or
 - (b) which has a realistic prospect of coming into existence or occurring.
- (3) For the purposes of (2):
 - (a) the existence of *cryptoasset inside information* may be based on an overall assessment of the factors existing at the relevant time;
 - (b) the notion of the intermediate step should not be interpreted as meaning that the magnitude of the effect of the set of circumstances or the event in question on the prices of the *relevant qualifying cryptoassets* concerned must be taken into consideration; and
 - (c) an intermediate step should be deemed to be *cryptoasset inside information* if it, by itself, meets the criteria laid down in regulation 18(2) of the *Cryptoassets Regulations*.

Information to be taken into account in the investment decision of a reasonable person

4.3.12 G Regulation 18(4)(d) of the *Cryptoassets Regulations* provides that information which, if it were made public, would be likely to have a significant effect on the price of a *relevant qualifying cryptoasset* or *related instrument* means information that a reasonable *person* would be likely to use as the basis, or part of the basis, of the *person's* investment decisions.

- 4.3.13 G Reasonable *persons* base their investment decisions on information already available to them. Therefore, the question whether, in making an investment decision, a reasonable *person* would be likely to take into account a particular piece of information should be appraised based on information that is already available. Such an assessment should take into consideration:
- (1) the anticipated impact of the information in light of the totality of the activities of the related *relevant person* and other *persons* seeking admission of the *relevant qualifying cryptoasset* to trading;
 - (2) the reliability of the source of information; and
 - (3) any other market variables likely to affect the *relevant qualifying cryptoasset* in the given circumstances.
- 4.3.14 G Information available after an investment decision has been taken can be used to check the presumption that the information available beforehand was price-sensitive. It should not be used to take action against *persons* who drew reasonable conclusions from that prior information available to them.
- 4.3.15 G The following factors may be taken into account when considering whether information would be likely to be used by a reasonable *person* as part of the basis of that *person's* investment decisions (the 'reasonable investor test'):
- (1) the fact that the significance of the information will vary widely between *relevant issuers, persons responsible for the offer or UK QCATP operators*, depending on factors such as their size, recent developments, and the market sentiment about them and the sector in which they operate; and
 - (2) the likelihood that a reasonable *person* will make investment decisions relating to the *relevant qualifying cryptoasset or related instrument* to maximise that *person's* economic self-interest.
- 4.3.16 G It is not possible to prescribe how the reasonable investor test will apply in all possible situations. Any assessment may need to take into consideration:
- (1) the anticipated impact of the information in light of the totality of the activities in relation to the *relevant qualifying cryptoasset*;
 - (2) the reliability of the source of the information; and
 - (3) other market variables likely to affect the *relevant qualifying cryptoasset or related instrument* in the given circumstances.
- 4.3.17 G Information which is likely to be considered relevant to a reasonable *person's* decision includes information which affects:
- (1) the assets and liabilities of the *relevant issuer, person responsible for the offer or UK QCATP operator*;

- (2) the performance, or the expectation of the performance, of the business of the *relevant issuer, person responsible for the offer* or *UK QCATP operator*;
- (3) the financial condition of the *relevant issuer, person responsible for the offer* or *UK QCATP operator*;
- (4) the course of the business of the *relevant issuer, person responsible for the offer* or *UK QCATP operator*;
- (5) major new developments in the business of the *relevant issuer, person responsible for the offer* or *UK QCATP operator*;
- (6) information previously disclosed to the market; and
- (7) major new developments in relation to the *relevant qualifying cryptoasset*.

Significant effect on price

- 4.3.18 G In determining whether information would be likely to have a significant effect on the price of a *relevant qualifying cryptoasset* or *related instrument*, a *relevant issuer, person responsible for the offer* or *UK QCATP operator* should be mindful that there is no figure (percentage change or otherwise) that can be set for them when determining what constitutes a significant effect on the price of the *relevant qualifying cryptoasset* or *related instrument*. This will vary between *relevant issuers, persons responsible for the offer* and *UK QCATP operators*.

4.4 Cryptoasset insider dealing

- 4.4.1 G *Cryptoasset insider dealing* means using *cryptoasset inside information* as prohibited by regulation 22 of the *Cryptoasset Regulations*.
- 4.4.2 G Regulation 22(1) of the *Cryptoassets Regulations* provides that a *person* described in regulation 22(4) and (5) of the *Cryptoassets Regulations* is prohibited from:
- (1) using the *cryptoasset inside information* by:
 - (a) acquiring or disposing of, or attempting to acquire or dispose of, a *relevant qualifying cryptoasset* or *related instrument* to which that information relates, for that *person's* own account or on the account of another, either directly or indirectly; or
 - (b) cancelling or amending, or attempting to cancel or amend, an order concerning a *relevant qualifying cryptoasset* or *related instrument* to which that information relates, for that *person's* own account or on the account of another, either directly or indirectly; and

- (2) making a recommendation to, or inducing, another person, on the basis of the *cryptoasset inside information*:
 - (a) to acquire or dispose of a *relevant qualifying cryptoasset* or *related instrument* to which that information relates; or
 - (b) to cancel or amend an order concerning a *relevant qualifying cryptoasset* or *related instrument* to which that information relates.
- 4.4.3 G Regulation 22(2) of the *Cryptoassets Regulations* provides that a *person* is prohibited from using or relying on, or attempting to use or rely on, a recommendation within the scope of regulation 22(1)(b) of the *Cryptoassets Regulations* if the *person* knows, or ought to have known, that the recommendation is made on the basis of *cryptoasset inside information*.
- 4.4.4 G Regulation 22(5) of the *Cryptoassets Regulations* provides that the prohibition against *cryptoasset insider dealing* applies, among other situations, to where a *person* who possesses *cryptoasset inside information* knows, or ought to have known, that the information is *cryptoasset inside information*.

Essential characteristics of cryptoasset insider dealing

- 4.4.5 G The essential characteristic of *cryptoasset insider dealing* consists in an unfair advantage being obtained from *cryptoasset inside information* to the detriment of third parties who are unaware of such information and, consequently, the undermining of the integrity of cryptoasset markets and investor confidence.

Descriptions of behaviour that amount to cryptoasset insider dealing

- 4.4.6 G The following are examples of behaviour that may amount to *cryptoasset insider dealing* under the *Cryptoassets Regulations*, but are not intended to form an exhaustive list:
- (1) front running/pre-positioning – that is, a transaction for a *person*'s own benefit, on the basis of and ahead of an order which they are to carry out with or for another (in respect of which information concerning the order is *cryptoasset inside information*, which takes advantage of the anticipated impact of the order on the cryptoasset market); and
 - (2) purchasing *relevant qualifying cryptoassets* with the knowledge of a forthcoming airdrop (as explained in *CRYPTO* 4.3.9G(7)) in relation to those cryptoassets which has not yet been publicly announced.

Recommending or inducing

- 4.4.7 G The following are examples of behaviour that might fall within the scope of regulation 22(1)(b) of the *Cryptoassets Regulations*:
- (1) A director of a *relevant issuer*, while in possession of *cryptoasset inside information*, instructs an *employee* of that issuer to sell a

relevant qualifying cryptoasset in respect of which the information is *cryptoasset inside information*.

- (2) A *person* recommends or advises a friend to engage in behaviour which, if they themselves engaged in it, would amount to *cryptoasset market abuse*.

Examples of cryptoasset insider dealing

- 4.4.8 G The following descriptions are intended to assist in understanding certain behaviours which may constitute *cryptoasset insider dealing* under the *Cryptoassets Regulations* and concern the definition of *cryptoasset inside information* relating to *relevant qualifying cryptoassets*:
- (1) X is an *employee* of a *UK QCATP operator*. X tells a friend, Y, about an upcoming initial exchange offering that has not been announced publicly and Y then uses that information to trade.
- (2) X is an *employee* of a *relevant issuer* A. A issues a *qualifying stablecoin* outside of the *UK* and has sought admission of that stablecoin on a *UK QCATP*. X knows about an unresolved *backing asset pool* shortfall that has not been disclosed publicly and sells their own holdings in the *qualifying stablecoin*.
- 4.4.9 G (1) The description in (2) is intended to assist in understanding certain behaviours which may constitute *cryptoasset insider dealing* under the *Cryptoassets Regulations* and concerns the definition of *cryptoasset inside information* relating to pending client orders.
- (2) A dealer on the trading desk of a *firm* accepts a very large order in respect of a *relevant qualifying cryptoasset* from a client to be executed in a particular *month*. Before executing the order, the dealer executes a trade for the *firm* and on their personal account on a *UK QCATP*, based on the expectation that they will be able to sell the *relevant qualifying cryptoasset* at profit due to the significant price increase that will result from the execution of their client's order. Both trades could constitute *cryptoasset insider dealing*.

Cryptoasset insiders: factors to take into account

- 4.4.10 G The following factors may be taken into account in determining whether a *person* who possesses *cryptoasset inside information* ought to know that it is *cryptoasset inside information* for the purposes of regulation 22(5) of the *Cryptoassets Regulations*:
- (1) if a normal and reasonable *person* in the position of the *person* who has *cryptoasset inside information* would know, or ought to know, that the *person* from whom they received it is a *cryptoasset insider*; and

- (2) if a normal and reasonable *person* in the position of the *person* who has *cryptoasset inside information* would know, or ought to know, that it is *cryptoasset inside information*.

- 4.4.11 G For the purposes of being categorised as a *cryptoasset insider* under regulation 22(5) of the *Cryptoassets Regulations*, the *person* concerned does not need to know that the information concerned is *cryptoasset inside information*.

Cryptoasset insider dealing and legitimate behaviours

- 4.4.12 G Under regulation 23 of the *Cryptoasset Regulations*, the *FCA* may make *rules* specifying circumstances in which a *person* who possesses *cryptoasset inside information* is not to be regarded as using that information and engaging in *cryptoasset insider dealing*. These *rules* and accompanying *guidance* are set out below at *CRYPTO* 4.4.13R to *CRYPTO* 4.4.20R.

- 4.4.13 R The fact that a legal *person* is or has been in possession of *cryptoasset inside information* does not mean that the legal *person* has used that information and has thus engaged in *cryptoasset insider dealing* on the basis of an acquisition or disposal, where that legal *person*:

- (1) has established, implemented and maintained adequate and effective internal arrangements and procedures that effectively ensure that neither the *person* who made the decision on the legal *person*'s behalf to acquire or dispose of *relevant qualifying cryptoassets* or *related instruments* to which the information relates, nor another *person* who may have had an influence on that decision, was in possession of the *cryptoasset inside information*; and
- (2) has not encouraged, made a recommendation to, induced or otherwise influenced the *person* who, on behalf of the legal *person*, acquired or disposed of *relevant qualifying cryptoassets* or *related instruments* to which the *cryptoasset inside information* relates.

- 4.4.14 R The fact that a *person* is in possession of *cryptoasset inside information* does not mean that the *person* has used that information and has thus engaged in *cryptoasset insider dealing* on the basis of an acquisition or disposal, where that *person*, for the *relevant qualifying cryptoasset* or *related instrument* to which that information relates:

- (1) is a *market maker*; or
- (2) is authorised to act as a counterparty, pursuing their legitimate business of dealing in *relevant qualifying cryptoassets* or *related instruments* (including entering into an agreement for the underwriting of an issue of *relevant qualifying cryptoassets* or *related instruments*).

- 4.4.15 G The following factors may be taken into account in determining whether a *person*'s behaviour is in the pursuit of legitimate business for the purposes of *CRYPTO* 4.4.14R, and are indications that it is:

- (1) the extent to which the relevant trading by the *person* is carried out in order to hedge a risk and, in particular, the extent to which it neutralises and responds to a risk arising out of the *person's* legitimate business;
 - (2) whether, in the case of a transaction on the basis of *cryptoasset inside information* about a client's transaction which has been executed, the reason for it being *cryptoasset inside information* is that information about the transaction is not, or is not yet, required to be published under any relevant regulatory or *UK QCATP* obligations; or
 - (3) whether, if the relevant trading by that *person* is connected with a transaction entered into or to be entered into with a client (including a potential client), the trading either has no impact on the price or there has been adequate disclosure to that client that trading will take place and they have not objected to it.
- 4.4.16 R The fact that a *person* is in possession of *cryptoasset inside information* does not mean that the *person* has used that information and has thus engaged in *cryptoasset insider dealing* on the basis of an acquisition or disposal where that *person*:
- (1) is authorised to execute orders on behalf of third parties; and
 - (2) the acquisition or disposal of *relevant qualifying cryptoassets* or *related instruments* to which the order relates is made to carry out such an order legitimately in the normal course of the exercise of that *person's* employment, profession or duties.
- 4.4.17 G For the purposes of *CRYPTO* 4.4.16R, the following factors may be taken into account in determining whether a *person's* behaviour in executing an order on behalf of another is carried out legitimately in the normal course of exercise of that *person's* employment, profession or duties, and are indications that it is:
- (1) whether the *person* has complied with the applicable provisions of *COBS* and *CRYPTO*;
 - (2) whether the *person* has agreed with their client that they will act in a particular way when carrying out, or arranging the carrying out of, the order;
 - (3) whether the *person's* behaviour was intended to facilitate or ensure the effective carrying out of the order; or
 - (4) whether, if the relevant trading by that *person* is connected with a transaction entered into or to be entered into with a client (including a potential client), the trading either has no impact on the price or there has been adequate disclosure to that client that trading will take place and they have not objected to it.

- 4.4.18 R The fact that a *person* is in possession of *cryptoasset inside information* does not mean that the *person* has used that information and has thus engaged in *cryptoasset insider dealing* on the basis of an acquisition or disposal where:
- (1) that *person* conducts a transaction to acquire or dispose of *relevant qualifying cryptoassets* or *related instruments*;
 - (2) that transaction is carried out in the discharge of an obligation that has become due in good faith and not to circumvent the prohibition against *cryptoasset insider dealing*; and
 - (3)
 - (a) that obligation results from an order placed or an agreement concluded before the *person* concerned possessed *cryptoasset inside information*; or
 - (b) that transaction is carried out to satisfy a legal or regulatory obligation that arose before the *person* concerned possessed *cryptoasset inside information*.
- 4.4.19 R The fact that a *person* uses their own knowledge that they have decided to acquire or dispose of *relevant qualifying cryptoassets* or *related instruments* in the acquisition or disposal of those *relevant qualifying cryptoassets* or *related instruments* does not of itself constitute use of *cryptoasset inside information*.
- 4.4.20 R Notwithstanding *CRYPTO* 4.4.13R to *CRYPTO* 4.4.19R, an infringement of the prohibition of *cryptoasset insider dealing* may still be deemed to have occurred if the *FCA* establishes that there was an illegitimate reason for the orders to trade, transactions or behaviours concerned.

4.5 Cryptoasset unlawful disclosure

- 4.5.1 G Cryptoasset unlawful disclosure means the prohibited disclosure of *cryptoasset inside information* as described in regulation 24 of the *Cryptoassets Regulations*, which provides as follows:
- (1) A *person* to whom this paragraph applies as a result of paragraph (3) or (4) is prohibited from disclosing that information to any other *person*, unless the disclosure is made in the normal course of the exercise of their employment, profession or duties.
 - (2) Where a *person* ('A') discloses a recommendation or inducement referred to in regulation 22(1)(b), which A knows or ought to know to have been based on *cryptoasset inside information*, the onward disclosure of that recommendation or inducement is prohibited, unless the disclosure is made in the normal course of the exercise of their employment, profession or duties.
 - (3) Paragraph (1) applies to a *person* who possesses *cryptoasset inside information* as a result of:

- (a) exercising administrative, management or supervisory functions of a relevant *person*;
 - (b) having a holding in the capital of:
 - (i) a *relevant issuer* of that *relevant qualifying cryptoasset* or *related instrument*;
 - (ii) a *person responsible for the offer* of that *relevant qualifying cryptoasset* or *related instrument*; or
 - (iii) a *person* who applied for or is seeking *admission to trading* on a *UK_QCATP* for that *relevant qualifying cryptoasset*;
 - (c) having access to the information through the exercise of their employment, profession or duties; or
 - (d) having acquired the information through criminal activity.
- (4) Paragraph (1) also applies to a *person*, other than one within paragraph (3), who knows, or ought to have known, that the information is *cryptoasset inside information*.

Descriptions of behaviour that indicates unlawful disclosure

- 4.5.2 G The following behaviours are indications of *cryptoasset unlawful disclosure*:
- (1) the director of a *relevant issuer* discloses *cryptoasset inside information* to a *person* in a social context or through private social media channels;
 - (2) an *employee* at a *UK_QCATP* tells a friend – who actively trades cryptoassets – about a new *relevant qualifying cryptoasset* that is going to be *admitted to trading* on that *UK_QCATP* before this information is made public;
 - (3) a developer working on a project involving a *relevant qualifying cryptoasset* privately messages a well-known community influencer to let them know about a major upgrade to that cryptoasset’s protocol before the upgrade is made public; or
 - (4) a *cryptoasset intermediary* discloses information about a large pending client order for a *relevant qualifying cryptoasset* to another market participant.

Descriptions of behaviour that does not indicate unlawful disclosure

- 4.5.3 G The following behaviour indicates that a *person* is acting in the normal exercise of their employment, profession or duties, if a *person* makes a disclosure of *cryptoasset inside information*:

- (1) to a government department, the Bank of England, the Competition and Markets Authority or any other *regulatory body* or authority for the purposes of fulfilling a legal or regulatory obligation; or
- (2) otherwise to such a body in connection with the performance of the functions of that body.

Factors to take into account in determining whether behaviour amounts to unlawful disclosure

- 4.5.4 G The following factors are to be taken into account in determining whether a disclosure was made by a *person* in the normal course of the exercise of their employment, profession or duties, and are indications that it was:
- (1) whether the disclosure is permitted by the rules of a *UK QCATP* or the *rules* of the *FCA*; or
 - (2) whether the disclosure is accompanied by the imposition of confidentiality requirements upon the *person* to whom the disclosure is made and is:
 - (a) reasonable and is to enable a *person* to perform the normal functions of their employment, profession or duties;
 - (b) reasonable and is (for example, to a professional adviser) for the purposes of facilitating or seeking or giving advice about a transaction;
 - (c) reasonable and is for the purpose of facilitating any commercial, financial or *investment* transaction in or related to a *relevant qualifying cryptoasset*; or
 - (d) in fulfilment of a legal obligation, including to employee representatives or trade unions acting on their behalf.

Examples of unlawful disclosure

- 4.5.5 G The following examples are intended to assist in understanding certain behaviours which may constitute *cryptoasset unlawful disclosure*:
- (1) X, a director at a *relevant issuer* has lunch with a friend Y, who has no connection with the *relevant issuer* or its advisers. X tells Y that the *relevant issuer* will soon be admitting a *relevant qualifying cryptoasset* to trading on a *UK QCATP*.
 - (2) A director of a *relevant issuer* asks a *cryptoasset intermediary* to sell some or all of that director's holdings in *relevant qualifying cryptoassets*. The *cryptoasset intermediary* tells a potential buyer that the seller is a director or reveals their identity, where that fact is *cryptoasset inside information*.

4.6 Cryptoasset market manipulation

Indicators of manipulative behaviour relating to false or misleading signals and to price securing

- 4.6.1 G *Cryptoasset market manipulation* means, as defined in regulation 19(1)(a) of the *Cryptoassets Regulations*, entering into a transaction, placing an order to trade or engaging in any other behaviour which:
- (1) gives, or is likely to give, false or misleading signals as to the supply of, demand for, or price of, a *relevant qualifying cryptoasset* or *related instrument*; or
 - (2) secures, or is likely to secure, the price of a *relevant qualifying cryptoasset* or *related instrument* at an abnormal or artificial level.
- 4.6.2 R For the purposes of applying regulation 19(1)(a)(i) of the *Cryptoassets Regulations*, and without prejudice to the forms of behaviour set out in regulation 19(2), the following non-exhaustive indicators, which do not necessarily, in themselves, constitute *cryptoasset market manipulation*, must be taken into account by *persons* entering into transactions or orders to trade:
- (1) the extent to which orders to trade given or transactions undertaken represent a significant proportion of the daily volume of transactions in the *relevant qualifying cryptoasset* or *related instrument* – in particular, when those activities lead to a significant change in their prices;
 - (2) the extent to which orders to trade given or transactions undertaken by persons with a significant buying or selling position in a *relevant qualifying cryptoasset* or *related instrument* lead to significant changes in their price;
 - (3) whether transactions undertaken lead to no change in beneficial ownership of a *relevant qualifying cryptoasset* or *related instrument*;
 - (4) the extent to which orders to trade given, transactions undertaken or orders cancelled include position reversals in a short period and represent a significant proportion of the daily volume of transactions in the *relevant qualifying cryptoasset* or *related instrument*, and might be associated with significant changes in the price of *relevant qualifying cryptoassets* or *related instruments*; and
 - (5) the extent to which orders to trade given change the representation of the offer prices in a *relevant qualifying cryptoasset* or *related instrument*, or more generally the representation of the order book available to market participants, and are removed before they are executed.

Factors to be taken into account: behaviour securing an abnormal or artificial price level

- 4.6.3 G The following factors are to be taken into account in determining whether a *person*'s behaviour amounts to manipulating transactions as described in regulation 19(1)(a)(ii) of the *Cryptoassets Regulations*:
- (1) the extent to which the *person* had a direct or indirect interest in the price or value of the *relevant qualifying cryptoasset* or *related instrument*;
 - (2) the extent to which price, rate or option volatility movements, and the volatility of these factors for the *relevant qualifying cryptoasset* or *related instrument* in question, are outside their normal intra-day, daily, weekly or monthly range; and
 - (3) whether a *person* has successively and consistently increased or decreased their offer or the price they have paid for a *relevant qualifying cryptoasset* or *related instrument*.

Factors to be taken into account: abusive squeezes

- 4.6.4 G The following factors are to be taken into account when determining whether a *person* has engaged in behaviour referred to in *CRYPTO* 4.6.2R(1) and (2) (commonly known as an 'abusive squeeze'):
- (1) the extent to which a *person* is willing to relax their control or other influence in order to help maintain an orderly market, and the price at which they are willing to do so – for example, behaviour is less likely to amount to an abusive squeeze if a person is willing to lend the *relevant qualifying cryptoasset* in question;
 - (2) the extent to which the *person*'s activity causes, or risks causing, settlement default by other market users on a multilateral basis and not just a bilateral basis – the more widespread the risk of multilateral settlement default, the more likely that an abusive squeeze has been effected; and
 - (3) the extent to which the spot or immediate cryptoasset market, compared to the forward cryptoasset market, is unusually expensive or inexpensive or the extent to which borrowing rates are unusually expensive or inexpensive.

Examples of manipulating transactions

- 4.6.5 G The following are examples of behaviour that may amount to manipulating transactions as described in regulation 19(1)(a)(ii) of the *Cryptoassets Regulations*:
- (1) A trader holds a short position that will show a profit if a particular *relevant qualifying cryptoasset*, which is currently a

component of an index, falls out of that index. The question of whether the *relevant qualifying cryptoasset* will fall out of the index depends on the closing price of that cryptoasset. The trader places a large *sell* order in the *relevant qualifying cryptoasset* just before the close of trading. The trader's purpose is to position the price of the *relevant qualifying cryptoasset* at a false, misleading, abnormal or artificial level so that it will drop out of the index so as to make a profit.

- (2) A fund manager's quarterly performance will improve if the valuation of their portfolio at the end of the quarter in question is higher rather than lower. The fund manager places a large order to *buy relevant qualifying cryptoassets*, which are also components of their portfolio, to be executed at or just before the close. The fund manager's purpose is to position the price of the *relevant qualifying cryptoasset* at a false, misleading, abnormal or artificial level.

Attempted market manipulation

- 4.6.6 G An attempt to engage in *cryptoasset market manipulation* should be distinguished from behaviour which is likely to result in *cryptoasset market manipulation* as both activities are prohibited under regulation 28 of the *Cryptoassets Regulations*. Such an attempt may include situations where the activity is started but is not completed – for example, as a result of failed technology or an instruction to trade which is not acted upon.

Unexecuted orders and behaviour occurring outside of a UK QCATP

- 4.6.7 G *Cryptoasset market manipulation* or attempted *cryptoasset market manipulation* may also consist in placing orders which may not be executed.
- 4.6.8 G *Cryptoasset market manipulation* or attempted *cryptoasset market manipulation* may also relate to the trading of *relevant qualifying cryptoassets* outside a UK QCATP – for example, peer-to-peer trading through decentralised finance, or the trading of a *relevant qualifying cryptoasset* on an *overseas qualifying cryptoasset trading platform*.

Indicators of manipulative behaviour relating to the employment of a fictitious device or any other form of deception or contrivance

- 4.6.9 G *Cryptoasset market manipulation* means, as defined in regulation 19(1)(b) of the *Cryptoassets Regulations*, entering into a transaction, placing an order to trade or any other activity or behaviour which affects or is likely to affect the price of a *relevant qualifying cryptoasset* or *related instrument*, while employing a fictitious device or any other form of deception or contrivance.
- 4.6.10 R For the purposes of applying regulation 19(1)(b) of the *Cryptoassets Regulations*, the following non-exhaustive indicators, which do not necessarily, in themselves, constitute *cryptoasset market manipulation*, must be taken into account by *persons* entering into transactions or orders to trade:

- (1) whether orders to trade given or transactions undertaken by *persons* are preceded or followed by dissemination of false or misleading information by the same *persons* or by *persons* linked to them; and
- (2) whether orders to trade are given or transactions are undertaken by *persons* before or after the same *persons* or *persons* linked to them produce or disseminate information recommending or suggesting investment strategies which are biased or demonstrably influenced by material interest.

4.6.11 R *CRYPTO* 4.6.10R is without prejudice to the forms of behaviour set out in regulation 19(2) of the *Cryptoassets Regulations* and summarised as follows:

- (1) exerting control over the supply or demand to influence prices or create unfair conditions;
- (2) using order placement or cancellation strategies to mislead market participants or disrupt the functioning of *UK QCATPs*; and
- (3) exploiting media influence to affect prices while concealing conflicts of interest from the public for personal gain.

Dissemination

4.6.12 G *Cryptoasset market manipulation* means, as defined in regulation 19(1)(c) of the *Cryptoassets Regulations*, disseminating information, including the dissemination of rumours, through the media, including the internet, or by any other means which:

- (1) gives, or is likely to give, false or misleading signals as to the supply of, demand for, or price of a *relevant qualifying cryptoasset* or *related instrument*; or
- (2) secures, or is likely to secure, the price of a *relevant qualifying cryptoasset* or *related instrument* at an abnormal or artificial level,

where the *person* who engaged in the dissemination knew, or ought to have known, that the information was false or misleading.

4.6.13 G The spreading of false or misleading information may consist in the invention of manifestly false information, but also the omission of material facts, as well as the knowingly inaccurate reporting of information. That form of *cryptoasset market manipulation* is particularly harmful to investors, because it causes them to base their investment decisions on incorrect or distorted information.

4.6.14 G The following factors can be taken into account in determining whether behaviour amounts to dissemination:

- (1) If a normal and reasonable *person* would know or ought to have known in all the circumstances that the information was false or misleading,

that indicates that the *person* disseminating the information knew or ought to have known that it was false or misleading.

- (2) If the individuals responsible for dissemination of information within an organisation could only know that the information was false or misleading if they had access to other information that was being held behind an *information barrier* or similarly effective arrangements, that indicates that the *person* disseminating did not know and could not reasonably be expected to have known that the information was false or misleading.

- 4.6.15 G (1) Paragraph (2) contains an example of behaviour that may amount to a *cryptoasset market manipulation* under regulation 19(1)(c) of the *Cryptoassets Regulations*.
- (2) A *person* posts false or misleading statements on social media that a public figure or influential market analyst has endorsed a *relevant qualifying cryptoasset*, where the *person* knows or ought to know that these statements are false or misleading.

4.7 Arrangements, systems and procedures for UK QCATP operators

Application and scope

- 4.7.1 G (1) Regulation 30(2) of the *Cryptoassets Regulations* requires, in relation to *relevant qualifying cryptoassets*, that *UK QCATP operators* establish and maintain effective arrangements, systems and procedures aimed at preventing, detecting and disrupting:
- (a) *cryptoasset insider dealing*;
 - (b) *cryptoasset market manipulation*;
 - (c) attempted *cryptoasset insider dealing*; and
 - (d) attempted *cryptoasset market manipulation*.
- (2) Regulation 30(4) of the *Cryptoassets Regulations* requires *UK QCATP operators*, when receiving information in a notification under regulation 30(3) of the *Cryptoassets Regulations* (see *CRYPTO 4.8.1G(2)*), to comply with any applicable *FCA rules*.
- 4.7.2 G Regulation 30(5) of the *Cryptoassets Regulations* provides that the *FCA* may make certain *rules*, including in relation to:
- (1) the design, scope and application of the arrangements, systems and procedures in regulation 30(2) of the *Cryptoassets Regulations*;
 - (2) notifications under regulation 30(3) of the *Cryptoassets Regulations*;

- (3) restrictions on onward transmission or use of information by the *UK QCATP operators* receiving a notification for the purposes of regulation 30(3) of the *Cryptoassets Regulations*; and
- (4) such matters related to regulation 30 of the *Cryptoassets Regulations* as the *FCA* considers appropriate.

4.7.3 G This section contains *rules* and *guidance* on:

- (1) the arrangements, systems and procedures for *UK QCATP operators* (in *CRYPTO* 4.7.5R to *CRYPTO* 4.7.19G);
- (2) additional requirements for the arrangements, systems and procedures for *large CATP operators* (in *CRYPTO* 4.7.20R to *CRYPTO* 4.7.23R);
- (3) the receipt and handling of notifications by *UK QCATP operators* (in *CRYPTO* 4.7.24R to *CRYPTO* 4.7.27R); and
- (4) related matters, such as audit and record keeping, for *UK QCATP operators* (in *CRYPTO* 4.7.28G to *CRYPTO* 4.7.33R).

4.7.4 R References to *cryptoasset market abuse* activities in this section refer only to:

- (1) *cryptoasset insider dealing*;
- (2) *cryptoasset market manipulation*;
- (3) attempted *cryptoasset insider dealing*; and
- (4) attempted *cryptoasset market manipulation*.

Overarching requirements for the arrangements, systems and procedures required for UK QCATP operators

4.7.5 R The arrangements, systems and procedures must:

- (1) ensure effective and ongoing monitoring of:
 - (a) all orders received and transmitted on the *qualifying cryptoasset trading platform*;
 - (b) the full range of trading activities on the *qualifying cryptoasset trading platform*, including all transactions executed on the *qualifying cryptoasset trading platform*; and
 - (c) activities and communications relating to a *qualifying cryptoasset* which is subject to an application to be *admitted to trading* on the *qualifying cryptoasset trading platform*;

- (2) enable the *UK QCATP operator* to analyse as quickly as practicable whether, on a case-by-case basis, a given order, transaction or activity is suspicious;
 - (3) enable the *UK QCATP operator* to prevent and/or disrupt any *cryptoasset market abuse* activity once detected; and
 - (4) enable the prompt and effective receipt and assessment of notifications of suspicious orders or transactions from *cryptoasset intermediaries* under regulation 30(3) of the *Cryptoassets Regulations*;
- 4.7.6 R (1) For the purposes of *CRYPTO* 4.7.5R(2), the *UK QCATP operator* must base its analysis on reasonable grounds.
- (2) Analysis that is based on speculation or presumption would not be based on reasonable grounds for the purposes of (1).
- 4.7.7 R The *UK QCATP operator* must ensure that its arrangements, systems and procedures:
- (1) include an appropriate level of human analysis; and
 - (2) employ software systems which assist with the prevention, detection and disruption of *cryptoasset market abuse* activities.
- 4.7.8 R A *UK QCATP operator* must establish and maintain the arrangements, systems and procedures irrespective of:
- (1) the capacity in which the order is placed or the transaction is executed; and
 - (2) the types of clients concerned.

Proportionality

- 4.7.9 R A *UK QCATP operator* must ensure that the arrangements, systems and procedures are appropriate and proportionate in relation to the scale, size and nature of its business activity.
- 4.7.10 R A *UK QCATP operator* must, upon request, provide the *FCA* with information to demonstrate compliance with *CRYPTO* 4.7.9R, including information on the level of automation put in place in such systems.

Further provision on detecting cryptoasset market abuse activities

- 4.7.11 R Without prejudice to the generality of *CRYPTO* 4.7.5R(1) and (2), a *UK QCATP operator* must ensure that the arrangements, systems and procedures, as a minimum:

- (1) provide for the analysis, individually and comparatively, of each and every transaction executed and order placed, modified, cancelled or rejected in the systems of the *qualifying cryptoasset trading platform*;
- (2) have facilities to replay the order book in order to analyse the activity of a trading session in the context of *algorithmic trading*, including high-frequency trading;
- (3) produce alerts in line with predefined parameters indicating activities requiring further analysis by the *UK QCATP operator* for the purposes of detecting potential *cryptoasset market abuse* activities;
- (4) monitor activities and communications made internally within the *UK QCATP operator* as well as externally, such as on social media, public forums and chat rooms, blogs, newsletters and podcasts; and
- (5) enable the detection of material and persistent dislocations between:
 - (a) the price of a *relevant qualifying cryptoasset* traded on its *qualifying cryptoasset trading platform*; and
 - (b) the price of the same *relevant qualifying cryptoasset* that is publicly available and traded on other markets which the *UK QCATP operator* reasonably considers to be material for price formation.

Further provision on preventing and disrupting cryptoasset market abuse

- 4.7.12 R The *UK QCATP operator* must ensure that the *qualifying cryptoasset trading platform* has in place:
- (1) arrangements, systems and procedures to halt, suspend or constrain trading;
 - (2) rules that set out options for disrupting *cryptoasset market abuse* activities, including the ability to:
 - (a) warn users of the *qualifying cryptoasset trading platform*;
 - (b) restrict the activities of users of the *qualifying cryptoasset trading platform*;
 - (c) increase surveillance and scrutiny of particular orders and transactions;
 - (d) suspend and remove *relevant qualifying cryptoassets* from the *qualifying cryptoasset trading platform*;
 - (e) offboard users of the *qualifying cryptoasset trading platform*; and

- (f) sanction users of the *qualifying cryptoasset trading platform*;
and
- (3) trading rules contributing to the prevention of *cryptoasset market abuse* activities.

Arrangements with clients

- 4.7.13 R A *UK QCATP operator* must establish and maintain arrangements, including, where appropriate, contractual agreements with clients, which allow that *UK QCATP operator* to prevent and disrupt *cryptoasset market abuse* activities, including the ability to take the actions set out in *CRYPTO 4.7.12R*.

Further provision on preventing, detecting and disrupting cryptoasset market abuse through internal controls

- 4.7.14 R A *UK QCATP operator* must have internal arrangements, systems and procedures to prevent, detect and disrupt *cryptoasset market abuse* activities, including:
- (1) *information barriers*, including barriers that limit the access that *employees* of the *UK QCATP operator* have to client orders to prevent *cryptoasset market abuse* activities, such as to prevent front running; and
 - (2) arrangements with *employees* to support any investigations into whether that *employee* has:
 - (a) acted in contravention of the *UK QCATP operator's* internal arrangements, systems and procedures; or
 - (b) undertaken *cryptoasset market abuse* activities.
- 4.7.15 R 'Front running' under *CRYPTO 4.7.14R(1)* is a transaction that:
- (1) is for a *person's* own benefit;
 - (2) is made on the basis of and ahead of an order which that *person* is to carry out with or for another (in respect of which information concerning the order is *cryptoasset inside information*); and
 - (3) takes advantage of the anticipated impact of the order on the market price.
- 4.7.16 R For the purposes of *CRYPTO 4.7.14R(2)*, a *UK QCATP operator's* arrangements with *employees* shall, where permitted by *data protection legislation*, include the ability to require an *employee* who is suspected of the activities in *CRYPTO 4.7.14R(2)(a)* and (b) to disclose details of any wallet addresses they own.
- 4.7.17 G A *UK QCATP operator* is also subject to:

- (1) personal account dealing arrangements in *CRYPTO* 5.8; and
- (2) conflicts of interest requirements in *CRYPTO* 6.3.4R and *CRYPTO* 6.3.5G.

Staff training

- 4.7.18 R A *UK QCATP operator* must, on a regular basis, organise and provide effective and comprehensive training to the staff involved in preventing, detecting and disrupting orders and transactions that could indicate the existence of *cryptoasset market abuse* activities, including the staff involved in processing orders and transactions.
- 4.7.19 R A *UK QCATP operator* must ensure that the training in *CRYPTO* 4.7.18R includes, as appropriate, information on:
- (1) handling and managing *cryptoasset inside information*;
 - (2) maintaining appropriate *information barriers* among relevant staff; and
 - (3) managing *cryptoasset inside information* disclosures to the market concerning initial exchange offerings.

Additional rules for large CATP operators

- 4.7.20 R In addition to (or as part of) the other requirements under *CRYPTO* 4.7, a *large CATP operator* must ensure its arrangements, systems and procedures:
- (1) include the effective and ongoing monitoring of orders or transactions of relevant wallets that are settled on a distributed ledger ('on-chain activity') to detect *cryptoasset market abuse* activity in accordance with *CRYPTO* 4.7.22R;
 - (2) enable compliance with the requirements for disclosure of information to other *large CATP operators* in accordance with *CRYPTO* 4.9;
 - (3) enable the prompt and effective receipt and assessment of information sent by other *large CATP operators* under *CRYPTO* 4.9; and
 - (4) ensure information received under *CRYPTO* 4.7.20R(3) is assessed in accordance with *CRYPTO* 4.7.5R(2).
- 4.7.21 R For the purposes of *CRYPTO* 4.7.20R(1), 'relevant wallets' means:
- (1) wallets that:
 - (a) are used to carry out trading activities, including placing orders or transactions on the *large CATP operator's qualifying cryptoasset trading platform*; and

- (b) have been identified as presenting a risk of *cryptoasset market abuse* activity by the arrangements, systems and procedures of the *large CATP operator*; and
- (2) any other wallets that are reasonably identifiable as being controlled by the same *person* or *group of persons* as the wallets in (1).

On-chain monitoring requirements for large CATP operators

4.7.22 R A *large CATP operator* must:

- (1) establish and maintain the ability to monitor on-chain activity; and
- (2) identify whether such on-chain activity could be linked to a *cryptoasset market abuse* activity on the *qualifying cryptoasset trading platform*, or itself constitute a *cryptoasset market abuse* activity.

4.7.23 G (1) The monitoring of on-chain activity may include the monitoring of wallet interactions, token flows and transaction patterns.

- (2) Methods for the monitoring of on-chain activity may include the use of blockchain analytics, wallet clustering and anomaly detection.

Notification of suspicious orders and transactions

4.7.24 R Subject to *CRYPTO 4.7.25R*, a *UK QCATP operator* must:

- (1) only use the notification, or information contained in the notification, received under regulation 30(3) of the *Cryptoassets Regulations* for the purposes of preventing, detecting or disrupting *cryptoasset market abuse* activity and for no other purpose; and
- (2) not transmit the notification, or information contained in the notification, to any third parties.

4.7.25 R A *UK QCATP operator* may use or transmit the notification, or information contained in the notification, where it is necessary to do so for the purposes of complying with its legal or regulatory obligations.

4.7.26 G Examples where it may be necessary for a *UK QCATP operator* to use or transmit the notification, or information contained in the notification, under *CRYPTO 4.7.25R* include:

- (1) transmitting such information to the *FCA* in accordance with *Principle 11* (Relations with regulators) or upon request by the *FCA*;
- (2) in the case of a *large CATP operator*, disclosing such information to other *large CATP operators* where it is required to do so under *CRYPTO 4.9*;
- (3) obtaining legal advice on its legal or regulatory obligations; and

- (4) transmitting or disclosing such information to a delegated party under *CRYPTO* 4.7.30G where that is necessary for compliance with its legal or regulatory obligations in connection with the relevant outsourced functions.

Secure receipt of notifications

- 4.7.27 R A *UK QCATP operator* must ensure that the mechanism used for receiving and storing notifications under regulation 30(3) of the *Cryptoassets Regulations* is:
- (1) adequately secure for the kind of information concerned; and
 - (2) capable of maintaining the completeness, integrity and confidentiality of the information concerned.

Data protection and other legal obligations

- 4.7.28 G (1) No obligations in *CRYPTO* 4.7 are to be interpreted in a manner which contravenes *data protection legislation*.
- (2) When considering the application of *CRYPTO* 4.7, *UK QCATP operators* should be mindful of their wider legal obligations, such as under competition law – in particular, where the information being shared is commercially sensitive.

Guidance on the relationship between *CRYPTO* 4.7 and Principle 11

- 4.7.29 G (1) *UK QCATP operators* are reminded of their obligations under *PRIN* 2.1.1R, including *Principle* 11 (Relations with regulators), which requires a *firm* to deal with its regulators in an open and cooperative way and disclose to the *FCA* appropriately anything relating to the *firm* of which the *FCA* would reasonably expect notice.
- (2) This includes notice of *cryptoasset market abuse* activity suspected by a *UK QCATP operator* where the *UK QCATP operator* reasonably concludes that it cannot adequately prevent, detect and disrupt the *cryptoasset market abuse* activity by appropriate measures available to it.

Delegation to another third party/another group entity

- 4.7.30 G Where a *UK QCATP operator* outsources, to a third party or to a legal *person* forming part of the same *group*, the performance of any functions to meet the requirements under *CRYPTO* 4.7, the *UK QCATP operator* will be subject to the *rules* and *guidance* in *SYSC* 8.

Audit and record keeping

- 4.7.31 R *UK QCATP operators* must ensure that the arrangements, systems and procedures required by *CRYPTO* 4.7 are:

- (1) regularly assessed, at least through an annually conducted audit and internal review, or sooner if there are relevant changes to the business, legal or regulatory environment or to the risk of *cryptoasset market abuse* activity occurring, and updated when necessary; and
- (2) clearly documented in writing, including any changes or updates to them, for the purposes of complying with the *rules* in *CRYPTO* 4 and the *cryptoasset market abuse* regime.

4.7.32 R *UK QCATP operators* must, for a period of 5 years, retain:

- (1) the information documenting the analysis carried out with regard to orders and transactions that could constitute *cryptoasset market abuse* activities, including where this information was reported internally within the *UK QCATP operator* and where this was reported externally to the *UK QCATP operator* by a *cryptoasset intermediary*;
- (2) records of notifications received from *cryptoasset intermediaries* and assessments made pursuant to *CRYPTO* 4.7.5R(4), and any action taken as a result; and
- (3) the documented information required under *CRYPTO* 4.7.31R(2).

4.7.33 R *UK QCATP operators* must provide to the *FCA* upon request the information and documents retained under *CRYPTO* 4.7.32R.

4.8 Arrangements, systems and procedures for cryptoasset intermediaries

Application and scope

- 4.8.1 G
- (1) Regulation 30(2) of the *Cryptoassets Regulations* requires, in relation to *relevant qualifying cryptoassets* and *related instruments*, *cryptoasset intermediaries* to establish and maintain effective arrangements, systems and procedures aimed at preventing, detecting and disrupting:
 - (a) *cryptoasset insider dealing*;
 - (b) *cryptoasset market manipulation*;
 - (c) attempted *cryptoasset insider dealing*; and
 - (d) attempted *cryptoasset market manipulation*.
 - (2) Regulation 30(3) of the *Cryptoassets Regulations* requires a *cryptoasset intermediary* to notify a *UK QCATP operator* without unnecessary delay where it reasonably suspects that an order or transaction in relation to any *relevant qualifying cryptoasset* or *related instrument*, whether placed or executed on, or outside, a *qualifying cryptoasset trading platform*, could constitute:
 - (a) *cryptoasset insider dealing*;

- (b) *cryptoasset market manipulation*;
 - (c) attempted *cryptoasset insider dealing*; or
 - (d) attempted *cryptoasset market manipulation*.
- 4.8.2 G Regulation 30(5) of the *Cryptoassets Regulations* provides that the *FCA* may make certain *rules*, including in relation to:
- (1) the design, scope and application of the arrangements, systems and procedures in regulation 30(2) of the *Cryptoassets Regulations*;
 - (2) notifications under regulation 30(3) of the *Cryptoassets Regulations*; and
 - (3) such matters related to regulation 30 of the *Cryptoassets Regulations* as the *FCA* considers appropriate.
- 4.8.3 G This section contains *rules* and *guidance* on:
- (1) the arrangements, systems and procedures for *cryptoasset intermediaries* (in *CRYPTO* 4.8.5R to *CRYPTO* 4.8.18G);
 - (2) notifications to *UK QCATP operators* in *CRYPTO* 4.8.19G to *CRYPTO* 4.8.33R; and
 - (3) related matters, such as audit and record keeping, in *CRYPTO* 4.8.34G to *CRYPTO* 4.8.39R.
- 4.8.4 R References to *cryptoasset market abuse* activities in this section refer only to:
- (1) *cryptoasset insider dealing*;
 - (2) *cryptoasset market manipulation*;
 - (3) attempted *cryptoasset insider dealing*; and
 - (4) attempted *cryptoasset market manipulation*.

Overarching requirements for the arrangements, systems and procedures

- 4.8.5 R The arrangements, systems and procedures must:
- (1) ensure effective and ongoing monitoring of the full range of trading activities undertaken by the *cryptoasset intermediary*, including all orders received or transmitted or transactions executed by the *cryptoasset intermediary*;
 - (2) enable the *cryptoasset intermediary* to analyse as quickly as practicable whether, on a case-by-case basis, a given order, transaction or activity is suspicious;

- (3) enable the *cryptoasset intermediary* to prevent and/or disrupt any *cryptoasset market abuse* activity once detected; and
 - (4) enable the *cryptoasset intermediary* to assess whether to notify the *UK QCATP operator(s)* without unnecessary delay under regulation 30(3) of the *Cryptoassets Regulations*.
- 4.8.6 R (1) For the purposes of *CRYPTO* 4.8.5R(2), the *cryptoasset intermediary* must base its analysis on reasonable grounds.
- (2) Analysis that is based on speculation or presumption would not be based on reasonable grounds for the purposes of (1).
- 4.8.7 R The *cryptoasset intermediary* must ensure that its arrangements, systems and procedures:
- (1) include an appropriate level of human analysis; and
 - (2) employ software systems which assist with the prevention, detection and disruption of *cryptoasset market abuse* activities.
- 4.8.8 R A *cryptoasset intermediary* must establish and maintain the arrangements, systems and procedures irrespective of:
- (1) the capacity in which the order is placed or the transaction is executed;
 - (2) the types of clients concerned; or
 - (3) whether the orders were placed or transactions executed on or outside a *qualifying cryptoasset trading platform*.

Proportionality

- 4.8.9 R A *cryptoasset intermediary* must ensure that the arrangements, systems and procedures are appropriate and proportionate in relation to the scale, size and nature of its business activity.
- 4.8.10 R A *cryptoasset intermediary* must, upon request, provide the *FCA* with information to demonstrate compliance with *CRYPTO* 4.8.9R, including information on the level of automation put in place in such systems.

Further provision on detecting cryptoasset market abuse activities

- 4.8.11 R Without prejudice to the generality of *CRYPTO* 4.8.5R(1) and (2), a *cryptoasset intermediary* must ensure that the arrangements, systems and procedures, as a minimum:
- (1) provide for the analysis, individually and comparatively, of each and every transaction executed and order placed, modified, cancelled or rejected in the systems of the *cryptoasset intermediary*;

- (2) have facilities to replay the order book in order to analyse the activity of a trading session in the context of *algorithmic trading*, including high-frequency trading;
- (3) produce alerts in line with predefined parameters indicating activities requiring further analysis by the *cryptoasset intermediary* for the purposes of detecting potential *cryptoasset market abuse* activities; and
- (4) monitor activities and communications made internally within the *cryptoasset intermediary* as well as externally, such as on social media, public forums and chat rooms, blogs, newsletters and podcasts.

Arrangements with clients

- 4.8.12 R A *cryptoasset intermediary* must establish and maintain arrangements, including, where appropriate, contractual agreements with clients, which allow the *cryptoasset intermediary* to prevent and disrupt *cryptoasset market abuse* activities, including the ability to offboard the client.

Further provision on preventing, detecting and disrupting cryptoasset market abuse internally

- 4.8.13 R A *cryptoasset intermediary* must have internal arrangements, systems and procedures to prevent, detect and disrupt *cryptoasset market abuse* activities, including:
- (1) *information barriers*, including barriers that limit the access that *employees* of the *cryptoasset intermediary* have to client orders to prevent *cryptoasset market abuse activities*, such as to prevent front running;
 - (2) effective arrangements to identify, prevent and manage conflicts of interest that could harm the interests of clients; and
 - (3) arrangements with *employees* to support any investigations into whether that *employee* has:
 - (a) acted in contravention of the *cryptoasset intermediary's* internal arrangements, systems and procedures; or
 - (b) undertaken *cryptoasset market abuse* activities.
- 4.8.14 R 'Front running' under *CRYPTO* 4.8.13R(1) is a transaction that:
- (1) is for a *person's* own benefit;
 - (2) is made on the basis of and ahead of an order which that *person* is to carry out with or for another (in respect of which information concerning the order is *cryptoasset inside information*); and

- (3) takes advantage of the anticipated impact of the order on the market price.
- 4.8.15 R For the purposes of *CRYPTO* 4.8.13R(3), a *cryptoasset intermediary's* arrangements with *employees* shall, where permitted by *data protection legislation*, include the ability to require an *employee* who is suspected of the activities in *CRYPTO* 4.8.13R(3)(a) and (b) to disclose details of any wallet addresses they own.
- 4.8.16 G A *cryptoasset intermediary* is also subject to:
- (1) personal account dealing arrangements in *CRYPTO* 5.8; and
 - (2) conflicts of interest requirements in *SYSC* 10.

Staff training

- 4.8.17 R *Cryptoasset intermediaries* must, on a regular basis, organise and provide effective and comprehensive training to the staff involved in preventing, detecting and disrupting orders and transactions that could indicate the existence of *cryptoasset market abuse* activities, including the staff involved in processing orders and transactions.
- 4.8.18 G A *cryptoasset intermediary* must ensure that the training in *CRYPTO* 4.8.17R includes, as appropriate, information on:
- (1) handling and managing *cryptoasset inside information*;
 - (2) maintaining appropriate *information barriers* among relevant staff; and
 - (3) managing *cryptoasset inside information* disclosures to the market concerning initial exchange offerings.

Notification of suspicious orders and transactions

- 4.8.19 G Under regulation 30(3) of the *Cryptoassets Regulations*, a *cryptoasset intermediary* may be required to notify more than one *UK QCATP operator*. For example, where the *relevant qualifying cryptoasset* is traded on multiple *qualifying cryptoasset trading platforms*, a *cryptoasset intermediary* may be required to notify each *UK QCATP operator* of those *qualifying cryptoasset trading platforms*.
- 4.8.20 G A *cryptoasset intermediary* should not wait for a particular number of suspicious orders or transactions to accumulate before notifying a *UK QCATP operator*. To do so would be inconsistent with the requirement to notify the *UK QCATP operator* without unnecessary delay.
- 4.8.21 R (1) Unless required to do so under regulation 30(3) of the *Cryptoasset Regulations*, a *cryptoasset intermediary* must not inform the *person* in respect of whom the notification will be submitted or anyone who is not required to know that the notification will be submitted.

- (2) A *cryptoasset intermediary* must have in place procedures to ensure that:
- (a) the *person* in respect of whom the notification was submitted; and
 - (b) anyone who does not need to know about the submission of the notification by virtue of their function or position, is not informed of the fact that a notification has been, will be or is intended to be submitted.

Guidance on when notification would and would not be required

- 4.8.22 G Regulation 30(3) of the *Cryptoassets Regulations* can apply in relation to transactions and orders which occurred in the past, where a suspicion has arisen in light of subsequent events and information.
- 4.8.23 G It will be necessary to delay a notification under regulation 30(3) of the *Cryptoassets Regulations* in circumstances where there is a reasonable belief that notifying the relevant *UK QCATP operator* without delay would prejudice an investigation into the *cryptoasset market abuse* activity, for instance, because the suspicion relates to the *UK QCATP operator* itself.
- 4.8.24 G *Cryptoasset intermediaries* should not notify *UK QCATP operators* of all orders received or transactions conducted that have triggered an internal alert. Such a requirement would be inconsistent with the requirement in *CRYPTO* 4.8.5R(2) to assess on a case-by-case basis whether there are reasonable grounds for suspicion.

Information to be included in the notification

- 4.8.25 R A *cryptoasset intermediary* must include in its notification any information of which the *cryptoasset intermediary* is aware and that is relevant and proportionate to disclose to facilitate or enable the prevention, detection or disruption of the *cryptoasset market abuse* activity of concern.
- 4.8.26 R Information under *CRYPTO* 4.8.25R includes, where relevant and depending on the nature of the suspected *cryptoasset market abuse* activity:
- (1) the names and identifiers of the *relevant qualifying cryptoasset* or *related instrument* and information identifying the orders and transactions in the *relevant qualifying cryptoasset* or *related instrument* for which suspicious activity has been detected;
 - (2) the time period or time stamp for when the suspicious activity occurred;
 - (3) a description of the order or transaction of concern, including the type of order and type of trading and the price and volume;

- (4) the type and nature of the *cryptoasset market abuse* activity suspected;
- (5) the reasons for suspecting the *cryptoasset market abuse* activity has taken place, is taking place or is likely to occur;
- (6) the verifiable evidence for holding any suspicions, including trends and anomalies in trading patterns or behaviours, and any analysis carried out;
- (7) the legal names, *LEI* or wallet address of, or any other appropriate means of identifying, any *person* in respect of whom the *cryptoasset intermediary's* verifiable suspicions relate; and
- (8) the capacity in which the *cryptoasset intermediary* submitting the notification operates, in particular when dealing on own account or executing orders on behalf of third parties.

Guidance on CRYPTO 4.8.25R

- 4.8.27 G (1) The question of whether information relating to the suspected *cryptoasset market abuse* activity of concern is relevant and proportionate must be assessed on a case-by-case basis, taking into account all the circumstances, including:
- (a) whether the disclosure contains sufficiently precise, substantiated and verifiable information to meet the purpose of the disclosure;
 - (b) whether the disclosure contains information beyond what is relevant and necessary to meet the purpose of the disclosure;
 - (c) whether the information contains any information that is merely speculative;
 - (d) the nature and seriousness of the suspicion and/or *cryptoasset market abuse* in question; and
 - (e) whether there is a need to act particularly quickly to address the *cryptoasset market abuse* activity identified.
- (2) Although information that falls within *CRYPTO* 4.8.25R is likely to be based on or comprise information ascertained as a result of the *cryptoasset intermediary's* arrangements, systems and procedures required by regulation 30(2) of the *Cryptoassets Regulations*, it may also include or comprise information from other sources of which the *cryptoasset intermediary* is aware.

Secure transmission of notification

- 4.8.28 R *Cryptoasset intermediaries* must ensure that the mechanism used for transmitting notifications is:

- (1) adequately secure for the kind of information concerned; and
- (2) capable of maintaining the completeness, integrity and confidentiality of the information concerned.

Subsequent information

- 4.8.29 R A *cryptoasset intermediary* must provide a *UK QCATP operator* with any relevant additional information of which it becomes aware after it has submitted the notification.

Exclusion of liability in connection with a notification

- 4.8.30 R Subject to *CRYPTO* 4.8.31R, a notification made to a *UK QCATP operator* pursuant to regulation 30(3) of the *Cryptoassets Regulations* does not give rise to:

- (1) a breach of any obligation of confidence owed by the *cryptoasset intermediary*; or
- (2) any other civil liability, on the part of that *cryptoasset intermediary*, to a *person* to whom the information disclosed relates.

- 4.8.31 R The exclusion of civil liability set out in *CRYPTO* 4.8.30R only applies to a *cryptoasset intermediary* notifying a *UK QCATP operator* under regulation 30(3) of the *Cryptoassets Regulations*, to the extent that the *cryptoasset intermediary* can demonstrate that:

- (1) it acted in good faith;
- (2) it reasonably suspected that the relevant order or transaction could constitute a *cryptoasset market abuse* activity;
- (3) it reasonably believed the information disclosed was relevant and proportionate to the purposes of detecting, preventing and disrupting the *cryptoasset market abuse* activity; and
- (4) the notification was transmitted in accordance with *CRYPTO* 4.8.28R.

Guidance on *CRYPTO* 4.8.30R

- 4.8.32 G The exclusion from liability in *CRYPTO* 4.8.30R only applies to the act of notifying a *UK QCATP operator*. As such, it does not apply with respect to civil liability that may arise out of the use of the information, including any action taken as a result of it, other than subsequent information disclosures under *CRYPTO* 4.8.29R.

No exclusion from liability under data protection legislation

- 4.8.33 R *CRYPTO* 4.8.30R does not apply to any civil liability arising under *data protection legislation*.

Data protection and other legal obligations

- 4.8.34 G (1) No obligations in *CRYPTO* 4.8 are to be interpreted in a manner which contravenes *data protection legislation*.
- (2) When considering the application of *CRYPTO* 4.8, *cryptoasset intermediaries* should be mindful of their wider legal obligations, such as under competition law – in particular, where the information being shared is commercially sensitive.

Guidance on the relationship between *CRYPTO* 4.8 and Principle 11

- 4.8.35 G (1) *Cryptoasset intermediaries* are reminded of their obligations under *PRIN* 2.1.1R, including *Principle* 11 (Relations with regulators), which requires a *firm* to deal with its regulators in an open and cooperative way and disclose to the *FCA* appropriately anything relating to the *firm* of which the *FCA* would reasonably expect notice.
- (2) This includes notice of *cryptoasset market abuse* activity suspected by a *cryptoasset intermediary* in situations where the *cryptoasset intermediary* reasonably concludes that it cannot adequately prevent, detect and disrupt the *cryptoasset market abuse* activity by appropriate measures available to it or by notifying a *UK QCATP operator* under regulation 30(3) of the *Cryptoassets Regulations*.

Delegation to another third party/another group entity

- 4.8.36 G Where a *cryptoasset intermediary* outsources, to a third party or to a legal *person* forming part of the same *group*, the performance of any functions to meet the requirements under *CRYPTO* 4.8, the *cryptoasset intermediary* will be subject to the *rules* and *guidance* in *SYSC* 8.

Audit and record keeping

- 4.8.37 R *Cryptoasset intermediaries* must ensure that the arrangements, systems and procedures required by *CRYPTO* 4.8 are:
- (1) regularly assessed, at least through an annually conducted audit and internal review, or sooner if there are relevant changes to the business, legal or regulatory environment or to the risk of *cryptoasset market abuse* activity occurring, and updated when necessary; and
- (2) clearly documented in writing, including any changes or updates to them, for the purposes of complying with the *rules* in *CRYPTO* 4 and the *cryptoasset market abuse* regime.
- 4.8.38 R *Cryptoasset intermediaries* must, for a period of 5 years, retain records of:
- (1) information shared with *UK QCATP operators* pursuant to regulation 30(3) of the *Cryptoassets Regulations*, the analysis for why this information was shared, and the facts and evidence underpinning this;

- (2) any information which *cryptoasset intermediaries* decided, after undertaking analysis, would not be shared with *UK QCATP operators*, the applicable analysis, and the related facts and evidence;
- (3) the information documenting the analysis carried out with regard to orders and transactions that could constitute *cryptoasset market abuse* activity;
- (4) records of identified conflicts of interest and the steps taken to address them under *CRYPTO* 4.8.13R(2); and
- (5) the documented information required under *CRYPTO* 4.8.37(2)R.

4.8.39 R *Cryptoasset intermediaries* must provide to the *FCA* upon request the information and documents retained under *CRYPTO* 4.8.38R.

4.9 Requirement for large CATP operators to disclose information for the purposes of detecting, preventing or disrupting cryptoasset market abuse

Disclosure obligation

- 4.9.1 G (1) Regulation 32(2) of the *Cryptoassets Regulations* requires certain *persons* (those listed in regulation 30(1)) to disclose information to relevant authorised cryptoasset *persons* for the purposes of disrupting, preventing and detecting *cryptoasset market abuse* in accordance with *FCA rules* (the ‘disclosure obligation’).
- (2) Regulation 32(4) of the *Cryptoassets Regulations* has the effect that the disclosure obligation applies only to *persons* and situations specified by *FCA rules*.
- (3) Regulation 32(4) also enables the *FCA* to make *rules* regarding other matters relating to the disclosure obligation including the content of the information to be disclosed, the mechanism for disclosure and the exclusion of civil liability.
- (4) *CRYPTO* 4.9 sets out these *rules*.

Persons to whom the disclosure obligation applies

4.9.2 R A *large CATP operator* is specified as a *person* to whom the disclosure obligation applies.

Situations in which the disclosure obligation applies

- 4.9.3 R The disclosure obligation applies when:
- (1) a *large CATP operator* has reasonable grounds to suspect that *cryptoasset market abuse* has occurred, is occurring or is likely to occur; and

- (2) it is necessary to disclose information of the kind specified in *CRYPTO* 4.9.9R to another *large CATP operator* in order to detect, prevent or disrupt the *cryptoasset market abuse* of concern.

Timing of the disclosure

- 4.9.4 R Where the disclosure obligation applies, the information required by *CRYPTO* 4.9.9R must be disclosed without unnecessary delay.

Authorised cryptoasset person to which information must be disclosed

- 4.9.5 R Where the disclosure obligation applies, the disclosure must be made to the *large CATP operator* to which it is necessary to disclose the information for the purpose of *CRYPTO* 4.9.3R.

Guidance on when disclosure would be required under the disclosure obligation in accordance with *CRYPTO* 4.9.2R to *CRYPTO* 4.9.5R

- 4.9.6 G For the avoidance of doubt, the disclosure obligation applies in relation to transactions and orders which occurred in the past, where a suspicion has arisen in light of subsequent events and information.
- 4.9.7 G Examples of where it would be necessary to disclose information under the disclosure obligation include where a *large CATP operator* has:
- (1)
 - (a) a reasonable belief that the other *large CATP operator* has in its possession additional information that is likely to materially assist it in detecting, preventing or disrupting the suspected *cryptoasset market abuse* of concern; and
 - (b) reasonably concluded that it is necessary to disclose information about the suspected *cryptoasset market abuse* of concern in order to enable that other *large CATP operator* to share that additional information with it;
 - (2)
 - (a) received information from the other *large CATP operator* that evidences a reasonable suspicion, on the basis of verifiable facts, that *cryptoasset market abuse* may have occurred, may be occurring or is likely to occur; and
 - (b) reasonably concluded that it is necessary to disclose information to the other *large CATP operator* to assist that operator with detecting, preventing or disrupting the suspected *cryptoasset market abuse* of concern;
 - (3)
 - (a) on the basis of verifiable facts, reasonable grounds to suspect that *cryptoasset market abuse* has occurred, may be occurring or is likely to occur in relation to a *qualifying cryptoasset* that is

admitted to trading on both its platform and the platform operated by the other *large CATP operator*; and

- (b) reasonably concluded that effective detection, prevention or disruption of the suspected *cryptoasset market abuse* of concern, in respect of the *qualifying cryptoassets* of concern, would be facilitated by action taken, or would require action to be taken, by the other *large CATP operator*; and
- (4) (a) taken steps, on the basis of verifiable facts, to prevent or disrupt suspected *cryptoasset market abuse* from taking place, such as terminating a business relationship with a particular *person* who the *large CATP operator* has reasonable grounds for suspecting is or was involved in the commission of *cryptoasset market abuse* on its exchange; and
- (b) reasonably concluded that the risk that the *person* could engage in *cryptoasset market abuse* on an exchange operated by the other *large CATP operator* is such that it is necessary and proportionate to inform that other *large CATP operator* of the steps it has taken, and the related circumstances, so that that other *large CATP operator* may consider whether it has grounds to take steps of its own in respect of that *person*.

- 4.9.8 G It would not be necessary or proportionate to disclose information where, in all the circumstances, disclosure is unlikely to assist with preventing or detecting the *cryptoasset market abuse* of concern, including when disclosure would be more likely than not to prejudice an investigation into the suspected *cryptoasset market abuse*.

Information that must be disclosed

- 4.9.9 R A *large CATP operator* must disclose under the disclosure obligation any information of which it is aware and that is relevant and proportionate to disclose to facilitate or enable the detection, prevention or disruption of the suspected *cryptoasset market abuse* of concern.

Guidance on CRYPTO 4.9.9R

- 4.9.10 G (1) The question of whether information relating to the suspected *cryptoasset market abuse* of concern is relevant and proportionate to disclose must be assessed on a case-by-case basis, taking into account all the circumstances, including:
- (a) whether the disclosure contains sufficiently precise, substantiated and verifiable information to meet the purpose of the disclosure;
 - (b) whether the disclosure contains information beyond what is strictly relevant and proportionate to meet the purpose of the disclosure;

- (c) whether the information contains any information that is merely speculative and not referable to verifiable facts;
 - (d) the nature and seriousness of the suspicion and/or market abuse in question; and
 - (e) whether there is a need to act particularly quickly to address the *cryptoasset market abuse* identified.
- (2) Although information that falls within *CRYPTO* 4.9.9R is likely to be based on or comprise information ascertained as a result of the *large CATP operator's* arrangements, systems and procedures required by *CRYPTO* 4.7R, it may also include or comprise information from other sources of which the *large CATP operator* is aware.
- (3) Information that may fall within *CRYPTO* 4.9.9R includes, depending on the nature of the suspected *cryptoasset market abuse*, and without limitation:
- (a) the names and identifiers of the *qualifying cryptoassets* and information identifying the orders and transactions in *qualifying cryptoassets* for which suspicious activity has been detected;
 - (b) the time period or time stamp for when the suspicious activity occurred;
 - (c) a description of the orders or transactions of concern, including the type of order and type of trading, and the price and volume;
 - (d) the type and nature of the *cryptoasset market abuse* suspected;
 - (e) the reasons for suspecting *cryptoasset market abuse* has taken place, is taking place or is likely to occur;
 - (f) the verifiable evidence for holding any suspicions, including trends and anomalies in trading patterns or behaviours;
 - (g) whether the behaviour has taken place on or off chain; and
 - (h) the legal names, *LEI* or wallet address of, or any other appropriate means of identifying, any *person* in respect of whom the *large CATP operator's* verifiable suspicions relate.

Restrictions on use of information received by virtue of the disclosure obligation

4.9.11 R Subject to *CRYPTO* 4.9.12R, a *large CATP operator* must:

- (1) only use information which has been disclosed to it by virtue of *CRYPTO* 4.9 for the purposes of detecting, preventing and disrupting *cryptoasset market abuse* activity and for no other purpose; and

- (2) not transmit information contained in the notification to any third parties.
- 4.9.12 R A *large CATP operator* may use or transmit information that has been disclosed to it by virtue of *CRYPTO 4.9* where it is necessary to do so for the purposes of complying with its legal or regulatory obligations.
- 4.9.13 G Examples where it may be necessary for a *large CATP operator* to use or transmit information under *CRYPTO 4.9.12R* include:
- (1) transmitting such information to the *FCA* in accordance with *Principle 11* (Relations with regulators) or upon request by the *FCA*;
 - (2) disclosing such information to other *large CATP operators* where it is required to do so under *CRYPTO 4.9*;
 - (3) obtaining legal advice on its legal or regulatory obligations; and
 - (4) transmitting or disclosing such information to a delegated party under *CRYPTO 4.7.30G* where that is necessary for compliance with its legal or regulatory obligations in connection with the relevant outsourced functions.

Secure transmission of disclosed information

- 4.9.14 R *Large CATP operators* must ensure that the mechanism used for transmitting information in compliance with the disclosure obligation is:
- (1) adequately secure for the kind of information concerned; and
 - (2) capable of maintaining the completeness, integrity and confidentiality of the information concerned.

Data protection and other legal obligations

- 4.9.15 G (1) No obligations in *CRYPTO 4.9* are to be interpreted in a manner which contravenes *data protection legislation*.
- (2) When considering the application of *CRYPTO 4.9*, *large CATP operators* should be mindful of their wider legal obligations, such as under competition law – in particular, where the information being shared is commercially sensitive.

Record keeping

- 4.9.16 R A *large CATP operator* must, for a period of 5 years, retain records of:
- (1) information disclosed to other *large CATP operators* pursuant to the disclosure obligation together with:

- (a) the facts and assessment that gave rise to the reasonable suspicion that *cryptoasset market abuse* had occurred, was occurring or was likely to occur;
 - (b) the reasons why it was considered necessary to share the information to detect, prevent or disrupt the *cryptoasset market abuse* of concern; and
 - (c) the reasons why the information shared was relevant and proportionate for the purposes of *CRYPTO 4.9.9R*;
- (2) any assessments leading to a decision to not disclose information to another *large CATP operator*, including, insofar as relevant:
- (a) reasons for concluding there was insufficient evidence to form reasonable grounds to suspect *cryptoasset market abuse*;
 - (b) reasons for concluding that it was not necessary to disclose information to detect, prevent or disrupt the *cryptoasset market abuse* of concern; and
 - (c) reasons for concluding that certain information would not meet the threshold of relevance or proportionality provided for in *CRYPTO 4.9.9R*; and
- (3) information received from other *large CATP operators* under the disclosure obligation, assessments made pursuant to *CRYPTO 4.7.20R*, and any action taken as a result.

4.9.17 G The *FCA* may request to see the records referred to in *CRYPTO 4.9.16R* under its information gathering powers and they must be provided to the *FCA* upon such a request.

Guidance on the relationship between disclosing to another large *CATP operator* under the disclosure obligation and disclosing to the *FCA* under Principle 11

- 4.9.18 G (1) *Large CATP operators* are reminded of their obligations under *PRIN 2.1.1R*, including *Principle 11* (Relations with regulators), which requires a *firm* to deal with its regulators in an open and cooperative way and disclose to the *FCA* appropriately anything relating to the *firm* of which the *FCA* would reasonably expect notice.
- (2) This includes notice of *cryptoasset market abuse* suspected by a *large CATP operator* where the *large CATP operator* reasonably concludes that the suspected *cryptoasset market abuse* of concern could not be adequately prevented, detected or disrupted by appropriate measures available to the *large CATP operator* either acting by itself or in conjunction with another *large CATP operator* with which information was shared, or is necessary to share, under the disclosure obligation.

Exclusion of liability in connection with a disclosure under the disclosure obligation

- 4.9.19 R Subject to *CRYPTO* 4.9.20R and *CRYPTO* 4.9.22R, a disclosure of information made or received by a *large CATP operator* pursuant to the disclosure obligation does not give rise to:
- (1) a breach of any obligation of confidence owed by the *large CATP operator*; or
 - (2) any other civil liability, on the part of that *large CATP operator*, to a *person* to whom the information disclosed relates.
- 4.9.20 R The exclusion of civil liability set out in *CRYPTO* 4.9.19R only applies to a *large CATP operator* disclosing information pursuant to the disclosure obligation to the extent that the *large CATP operator* can demonstrate:
- (1) it acted in good faith;
 - (2) it reasonably believed that the disclosure was necessary to detect, prevent, or disrupt the suspected *cryptoasset market abuse* of concern;
 - (3) it reasonably believed that the information disclosed was relevant and proportionate to the purposes of detecting, preventing and disrupting the suspected *cryptoasset market abuse* of concern; and
 - (4) the information was disclosed in accordance with *CRYPTO* 4.9.14R.
- 4.9.21 G The exclusion of liability in *CRYPTO* 4.9.19R only applies to the act of disclosing or receiving information. As such, it does not apply with respect to civil liability that may arise out of the use of the information, including any action taken as a result of it, other than further disclosures of information under the disclosure obligation.

No exclusion from liability under data protection legislation

- 4.9.22 R *CRYPTO* 4.9.19R does not apply to any civil liability arising under *data protection legislation*.

4.10 Public disclosure of cryptoasset inside information

Obligation to disclose under regulation 26 of the Cryptoassets Regulations

- 4.10.1 G (1) Under regulation 26 of the *Cryptoassets Regulations*, a *relevant person* ('A') must, where required to do so by *FCA rules*, inform the public of *cryptoasset inside information* that directly concerns A:
- (a) as soon as possible; and
 - (b) in a manner that enables fast access as well as complete, correct and timely assessment of the information by the public.

- (2) The *FCA* may make designated activity *rules*:
 - (a) specifying the *relevant persons* to whom regulation 26 applies;
 - (b) concerning the form, type, timing and technical means of disclosure required; and
 - (c) in relation to the application of regulation 26 as the *FCA* considers appropriate.

Application of regulation 26 of the Cryptoassets Regulations

4.10.2 R Regulation 26 of the *Cryptoassets Regulations* applies to the following *relevant persons*:

- (1) a *relevant issuer*;
- (2) a *person responsible for the offer*; and
- (3) a *UK QCATP*.

4.10.3 G (1) For the purposes of regulation 26, *cryptoasset inside information* can directly concern a *relevant issuer*, a *person responsible for the offer* and/or a *UK QCATP* where it relates to a *relevant qualifying cryptoasset* of which they are:

- (a) a *relevant issuer*;
- (b) a *person responsible for the offer*; or
- (c) a *UK QCATP* on which the *relevant qualifying cryptoasset* is *admitted to trading* or subject to an application seeking *admission to trading*.

(2) For example:

- (a) If a *relevant issuer* hires a third party to design a *relevant qualifying cryptoasset* and subsequently becomes aware that the third party's work introduced a code vulnerability, this would directly concern that *relevant issuer*.
- (b) If a *UK QCATP* outsources its custody infrastructure to a third-party provider and later discovers that an outage at the provider created a material risk of delayed or failed settlement for a *relevant qualifying cryptoasset admitted to trading* by that *UK QCATP*, this issue would directly concern that *UK QCATP*.
- (3) Regulation 26 does not, of itself, create an obligation to seek out and obtain inside information that is not already in the possession of the *relevant issuer*, *person responsible for the offer* and *UK QCATP operator*.

- 4.10.4 G In relation to decisions whether to publicly disclose *cryptoasset inside information* in accordance with regulation 26, *relevant issuers, persons responsible for the offer* and *UK QCATP operators* and their advisers are best placed to make an initial assessment of whether particular information amounts to *cryptoasset inside information*. The decision as to whether a piece of information is *cryptoasset inside information* may be finely balanced and the *relevant issuer, person responsible for the offer* or *UK QCATP operator* (with the help of its advisers) will need to exercise its judgement.
- 4.10.5 G A *relevant issuer, a person responsible for the offer* and a *UK QCATP operator* should carefully and continuously monitor whether changes in their circumstances or the circumstances relating to the *relevant qualifying cryptoasset* are such that the disclosure obligation in regulation 26(1) applies.

Manner, form and technical means of disclosure under regulation 26 of the Cryptoassets Regulations

- 4.10.6 R Information published to comply with regulation 26 must be published on the website of the *relevant issuer, person responsible for the offer* or *UK QCATP operator*.
- 4.10.7 R A *relevant issuer, a person responsible for the offer* and a *UK QCATP operator* must, for the purposes of *CRYPTO* 4.10.6R:
- (1) ensure that the *cryptoasset inside information* is in the form of a downloadable written statement and that the language used in that statement to describe the *cryptoasset inside information* is clear, precise and not misleading; and
 - (2) post and maintain on its website, for a period of at least 5 years, all *cryptoasset inside information* it is required to disclose publicly.
- 4.10.8 R *Cryptoasset inside information* disclosed on a website referred to in *CRYPTO* 4.10.6R must:
- (1) be accessible on a non-discriminatory basis and free of charge;
 - (2) be located in an easily identifiable section of the website; and
 - (3) clearly indicate the date and time of disclosure and be organised in chronological order.
- 4.10.9 R A *relevant issuer, a person responsible for the offer* and a *UK QCATP operator* does not have to comply with *CRYPTO* 4.10.6R, *CRYPTO* 4.10.7R or *CRYPTO* 4.10.8R where it does not have a website.
- 4.10.10 G Regulation 26 requires a *relevant issuer, a person responsible for the offer* and a *UK QCATP operator* to make disclosures in a manner that enables fast access to, as well as complete, correct and timely assessment of, the information by the public. Complying with this standard is likely to require

that other channels of dissemination are used in addition to disclosure on a website referred to in *CRYPTO* 4.10.6R.

- 4.10.11 G (1) A *relevant issuer*, a *person responsible for the offer* or a *UK QCATP operator* may consider communicating *cryptoasset inside information*, directly or indirectly, using the following forms of media, in each case subject to meeting the conditions of regulation 26:
- (a) traditional media;
 - (b) social media permitting publication in written form;
 - (c) web-based platforms which permit publication of news relating to a *relevant issuer*, a *person responsible for the offer* and a *UK QCATP operator*; and
 - (d) the website of the *UK QCATP operator*, where the related *relevant qualifying cryptoasset* is traded and where it provides this service.
- (2) The *FCA* would expect a *relevant issuer*, a *person responsible for the offer* or a *UK QCATP operator* to use a communication channel of this form only where it is reasonably satisfied that the channel is one on which the public can reasonably rely.
- 4.10.12 G Disseminating *cryptoasset inside information* through social media or web-based platforms where the social media or web-based platform does not ensure that the *cryptoasset inside information* is accessible to all users, or where the social media or web-based platform restricts access to users, would not comply with regulation 26.
- 4.10.13 R Where publication takes place on social media, web-based platforms or the website of a *UK QCATP*, the *relevant issuer*, the *person responsible for the offer* and the *UK QCATP operator* must include a link to the written statement published on their website in accordance with *CRYPTO* 4.10.7R(1).
- 4.10.14 R In complying with regulation 26, a *relevant issuer*, a *person responsible for the offer* and a *UK QCATP operator* must ensure that:
- (1) any communications made to a third party to enable the onward dissemination of *cryptoasset inside information* for the purposes of regulation 26 are transmitted using electronic means that maintain the completeness, integrity and confidentiality of the information during the transmission; and
 - (2) the information disseminated to the public clearly identifies:
 - (a) that the information communicated is *cryptoasset inside information*;

- (b) the identity of the *relevant issuer*, the *person responsible for the offer* and the *UK QCATP operator* (full legal name);
- (c) the identity of the *person* making the notification: name, surname, and position within the *relevant issuer*, the *person responsible for the offer* and the *UK QCATP operator* (where relevant);
- (d) the subject matter of the *cryptoasset inside information*; and
- (e) the date and time of the communication.

4.10.15 R A *relevant issuer*, a *person responsible for the offer* and a *UK QCATP operator* must ensure completeness, integrity and confidentiality by remedying any failure or disruption in the communication of *cryptoasset inside information* without delay.

Uploading to the FCA-owned centralised repository

- 4.10.16 R A *relevant issuer*, a *person responsible for the offer* and a *UK QCATP operator* must, for the purposes of regulation 26:
- (1) subsequently upload the *cryptoasset inside information* as soon as possible to the *FCA-owned centralised repository*; and
 - (2) when uploading that *cryptoasset inside information*, include the following identifying information:
 - (a) the name of, and any *LEI* that is included on the *GLEIF Global LEI Index* for, the *relevant issuer*, *person responsible for the offer* or *UK QCATP operator* that is uploading the *cryptoasset inside information*; and
 - (b) the name(s) of, and the *digital token identifier(s)* for, the *qualifying cryptoasset(s)* concerned.

Separation for marketing

4.10.17 R A *relevant issuer*, a *person responsible for the offer* and a *UK QCATP operator* must not combine the disclosure of *cryptoasset inside information* to the public with the marketing of its activities.

Delayed disclosure of cryptoasset inside information

- 4.10.18 G (1) Regulation 27(1) of the *Cryptoassets Regulations* provides that a *relevant person* may delay the public disclosure of *cryptoasset inside information* in accordance with *FCA rules*.
- (2) Regulation 27(2) of the *Cryptoassets Regulations* provides that the *FCA* may make *rules* concerning:

- (a) the form, type, timing of and arrangements for notifications to delay disclosure;
 - (b) the conditions under which disclosure may be delayed;
 - (c) the conditions or circumstances when disclosure would need to be made; and
 - (d) such matters relating to that regulation as the *FCA* considers appropriate.
- 4.10.19 R A *relevant issuer, person responsible for the offer* or UK *QCATP operator* may, on its own responsibility, delay disclosure of *cryptoasset inside information*, provided that all the following conditions are met:
- (1) immediate disclosure is likely to prejudice the legitimate interests of the *relevant issuer, person responsible for the offer* or UK *QCATP operator*;
 - (2) delay of disclosure is not likely to mislead the public; and
 - (3) the *relevant issuer, person responsible for the offer* or UK *QCATP operator* is able to ensure the confidentiality of that information.
- 4.10.20 R In the case of an ongoing process that occurs in stages and that is intended to bring about or that results in a particular circumstance or a particular event, a *relevant issuer, person responsible for the offer* or UK *QCATP operator* may, on its own responsibility, delay the public disclosure of inside information relating to this process, subject to *CRYPTO* 4.10.19R.
- 4.10.21 G For the purposes of applying the requirement in *CRYPTO* 4.10.19R(1), legitimate interests may, in particular, relate to the following circumstances, which are not intended to be exhaustive:
- (1) There are ongoing negotiations, or related elements, in relation to admission of a *relevant qualifying cryptoasset* to trading, where, if disclosed, the outcome of those negotiations would affect the price of the *relevant qualifying cryptoasset* itself.
 - (2) Where a *relevant issuer* is in discussions to make changes relating to a blockchain fork (see *CRYPTO* 4.3.9G(5)), the *relevant issuer* may wish to keep this information confidential until a final decision has been reached to avoid volatility in the price of a *qualifying cryptoasset*.
 - (3) Where, in the case of a security vulnerability, immediate disclosure would prejudice the ability of the *relevant issuer, person responsible for the offer* or UK *QCATP operator* to take effective measures to remediate that vulnerability.
- 4.10.22 R Where disclosure of *cryptoasset inside information* has been delayed in accordance with *CRYPTO* 4.10.19R or *CRYPTO* 4.10.20R, and the

confidentiality of that information is no longer ensured, the *relevant issuer, person responsible for the offer* or *UK QCATP operator* must disclose that information to the public as soon as possible under regulation 26 and in accordance with these *rules*. This includes situations where a rumour explicitly relates to *cryptoasset inside information*, the disclosure of which has been delayed in accordance with *CRYPTO 4.10.19R* or *CRYPTO 4.10.20R*, and the rumour is sufficiently accurate to indicate that the confidentiality of that information is no longer ensured.

- 4.10.23 G Where there is press speculation or market rumour regarding a *relevant issuer, person responsible for the offer* or *UK QCATP operator*, the *relevant issuer, person responsible for the offer* or *UK QCATP operator* should assess whether a disclosure obligation arises under regulation 26(1) of the *Cryptoassets Regulations*. To do this, the *relevant issuer, person responsible for the offer* or *UK QCATP operator* will need to carefully assess whether the speculation or rumour has given rise to a situation where it has *cryptoasset inside information*.
- 4.10.24 G The knowledge that press speculation or market rumour is false may not amount to *cryptoasset inside information*. If it does amount to *cryptoasset inside information*, the *FCA* expects that there may be cases where a *relevant issuer, person responsible for the offer* or *UK QCATP operator* would be able to delay disclosure in accordance with *CRYPTO 4.10.19R* or *CRYPTO 4.10.20R*.
- 4.10.25 R Where a *relevant issuer, person responsible for the offer* or *UK QCATP operator* has delayed the disclosure of *cryptoasset inside information* in accordance with the conditions in *CRYPTO 4.10.19R*, it must ensure the accessibility, readability and maintenance in a durable medium of all the following information:
- (1) the reason(s) for the delayed disclosure of *cryptoasset inside information*;
 - (2) the dates and times when:
 - (a) the *cryptoasset inside information* first existed within the *relevant issuer, person responsible for the offer* or *UK QCATP operator*;
 - (b) the decision to delay the disclosure of *cryptoasset inside information* was made; and
 - (c) the *relevant issuer, person responsible for the offer* or *UK QCATP operator* is likely to disclose the *cryptoasset inside information*;
 - (3) the identity, position and function of the person(s) within the *relevant issuer, person responsible for the offer* or *UK QCATP operator* responsible for:

- (a) deciding to delay the disclosure of the *cryptoasset inside information*, and deciding about the start of the delay and its likely end;
 - (b) ensuring the ongoing monitoring of the conditions for the delay of the disclosure of the *cryptoasset inside information*;
 - (c) deciding about the disclosure of the *cryptoasset inside information*; and
 - (d) providing to the *FCA* the information about the delayed disclosure;
- (4) evidence of the initial fulfilment of the conditions in *CRYPTO* 4.10.19R and of any change in that fulfilment during the delay period, including:
- (a) the information barriers which have been put in place internally and with regard to third parties to prevent access to *cryptoasset inside information* by persons other than those who require it for the normal exercise of their employment, profession or duties within the *relevant issuer, person responsible for the offer* or *UK QCATP operator*; and
 - (b) the arrangements put in place where the confidentiality of the *cryptoasset inside information* is no longer ensured; and
- (5) a complete record of the *cryptoasset inside information* that is subject to the delayed disclosure, including, once the *cryptoasset inside information* is publicly disclosed, the reference number (where the dissemination system used assigns one), the duration of the delay, and the date and time of the public disclosure of the *cryptoasset inside information*.
- 4.10.26 R A *relevant issuer, person responsible for the offer* or *UK QCATP operator* must make the information listed in *CRYPTO* 4.10.25R available to the *FCA* on request, in a form specified by the *FCA*.
- 4.10.27 R For the purposes of *CRYPTO* 4.10.25R, ‘durable medium’ means any instrument which stores information in a way that is accessible for future reference for a period of time adequate for the purposes of the information and allows the unchanged reproduction of the information stored.
- 4.11 Legitimate cryptoasset market practices**
- 4.11.1 G (1) Regulations 23(1)(a), 25(1)(a) and 29(1)(a) of the *Cryptoassets Regulations* provide exclusions applicable to the prohibitions in regulations 22 (insider dealing), 24 (disclosure of inside information) and 28 (market manipulation) respectively.

- (2) The exclusions referred to in (1) apply to conduct specified as a *legitimate cryptoasset market practice* in rules made under regulation 34(1) of the *Cryptoassets Regulations*.
- (3) A *person* does not contravene the prohibitions in regulations 22, 24 or 28 where the conduct that would otherwise fall within those regulations is specified as a *legitimate cryptoasset market practice* in relation to the relevant prohibition.

- 4.11.2 G The *rules* in this section specify the market practices listed in the first column of the table below as *legitimate cryptoasset market practices* for the purpose of the prohibitions in the *Cryptoassets Regulations* listed in the second column of the table.

	Legitimate cryptoasset market practice	Prohibition
(1)	Burning	(a) regulation 22 (insider dealing); (b) regulation 24 (disclosure of inside information); and (c) regulation 28 (market manipulation).
(2)	Crypto-stabilisation	(a) regulation 22 (insider dealing); (b) regulation 24 (disclosure of inside information); and (c) regulation 28 (market manipulation).

Burning

- 4.11.3 G (1) The following *rules* and *guidance* are about *burning*.
- (2) *Burning* is the process by which a cryptoasset is permanently removed from circulation on a blockchain.
- (3) Some cryptocurrency developers intentionally *burn* cryptoassets for the purpose of supporting the effective functioning of the market in that cryptoasset by reducing supply. This is not dissimilar to ‘buy-back programmes’ in traditional finance, where entities trade in their own shares.
- 4.11.4 R Subject to *CRYPTO* 4.11.5R, *burning* is specified as a *legitimate cryptoasset market practice* for the purpose of the prohibitions in regulations 22, 24 and 28 of the *Cryptoassets Regulations*.
- 4.11.5 R The prohibitions in regulations 22, 24 and 28 of the *Cryptoassets Regulations* do not apply to the activity of *burning* only where:

- (1) the *burning* is done by a *relevant person*; and
- (2) that *relevant person* ensures that:
 - (a) for *burning* that is a feature of the *relevant qualifying cryptoasset* or its underlying technology, the *burning* is conducted in accordance with a defined framework or protocol, the full details of which have been publicly disclosed;
 - (b) for *burning* conducted on an ad hoc basis:
 - (i) full details of the *burning* process are disclosed to the public prior to the start of the *burning* process, including:
 - (A) the purpose of the *burning*;
 - (B) the maximum number of units of the *relevant qualifying cryptoasset* allocated to the *burning*;
 - (C) the maximum fiat value of the *relevant qualifying cryptoasset* to be burned; and
 - (D) the period allocated for the *burning*;
 - (ii) transactions which are part of the *burning* process are:
 - (A) recorded; and
 - (B) subsequently disclosed to the public, except where the existence of the transaction can be observed directly on the blockchain; and
 - (iii) each instance of *burning* of a *relevant qualifying cryptoasset* completed as part of the *burning* process is:
 - (A) recorded; and
 - (B) subsequently disclosed to the public, except where the instance of *burning* can be observed directly on the blockchain; and
 - (c) the sole purpose of the activity is to support the effective functioning of the market in the *relevant qualifying cryptoasset* by reducing the amount of the *relevant qualifying cryptoassets* which are in circulation.

4.11.6 G For the purposes of *CRYPTO* 4.11.5R, a disclosure would be made publicly where it is made:

- (1) as part of an applicable *QCDD* or *supplementary disclosure document* for the *relevant qualifying cryptoasset*; or
- (2) in accordance with *CRYPTO* 4.10.

Crypto-stabilisation

- 4.11.7 G The following *rules* and *guidance* are about crypto-stabilisation.
- 4.11.8 R For the purposes of this section, ‘crypto-stabilisation’ means a purchase of, or offer to purchase, *relevant qualifying cryptoassets*, or a transaction in *related instruments* equivalent to such a purchase or offer, which is undertaken:
- (1) in the context of a distribution of such *relevant qualifying cryptoassets* or *related instruments*;
 - (2) exclusively for supporting the market price of those *relevant qualifying cryptoassets* or *related instruments*;
 - (3) for a predetermined period of time; and
 - (4) due to a selling pressure in such *relevant qualifying cryptoassets* or *related instruments*.
- 4.11.9 R Subject to *CRYPTO* 4.11.10R, crypto-stabilisation is specified as a *legitimate cryptoasset market practice* for the purpose of the prohibitions in regulations 22, 24 and 28 of the *Cryptoassets Regulations*.
- 4.11.10 R The prohibitions in regulations 22, 24 and 28 of the *Cryptoassets Regulations* do not apply to the activity of crypto-stabilisation only where the crypto-stabilisation is done by a *relevant person* and that *relevant person* ensures that:
- (1) the crypto-stabilisation is carried out for a limited period as follows:
 - (a) in the case of a distribution in the form of an initial coin offer which is publicly announced, the limited period starts on the date of commencement of trading of the *relevant qualifying cryptoasset* or *related instrument* on the *UK QCATP* concerned and ends no later than 30 calendar *days* after that date; or
 - (b) in the case of a distribution in the form of a secondary coin offer, the limited period starts on the *day* when the offer is publicly disclosed and ends no later than 30 calendar *days* after that date;
 - (2) transactions which are part of the crypto-stabilisation process are:
 - (a) recorded;

- (b) subsequently disclosed to the public, except where the existence of the trade can be observed directly on the blockchain; and
 - (c) carried out in compliance with the applicable rules of the *UK QCATP* on which the *relevant qualifying cryptoasset* is, or is to be, *admitted to trading*, including any rules concerning public disclosure and trade reporting; and
- (3) the records referred to in (2)(a) are retained for a period of 5 years and made available to the *FCA* on request.

4.12 Cryptoasset insider lists

Application and scope

- 4.12.1 G (1) Regulation 31(1) of the *Cryptoassets Regulations* provides that a *relevant person* must, where required to do so under any *FCA rules* made by virtue of (2):
- (a) draw up a *cryptoasset insider list*;
 - (b) maintain and update that *cryptoasset insider list*; and
 - (c) provide that *cryptoasset insider list* to the *FCA* upon its request.
- (2) Regulation 31(2) of the *Cryptoassets Regulations* provides that the *FCA* may make *rules*:
- (a) specifying the *relevant persons* to whom regulation 31 applies;
 - (b) concerning the form, content, maintenance, updating and recording of a *cryptoasset insider list* for the purposes of (1), including how and when a *relevant person* must provide a *cryptoasset insider list* to the *FCA*; and
 - (c) on such matters related to regulation 31 as the *FCA* considers appropriate.
- 4.12.2 R In accordance with regulation 31(2)(a), the *rules* in this section apply to:
- (1) a *relevant issuer*;
 - (2) a *person responsible for the offer*; and
 - (3) a *UK QCATP operator*.

Requirement to draw up cryptoasset insider lists, and form and content of cryptoasset insider lists

- 4.12.3 R *A relevant issuer, person responsible for the offer or UK QCATP operator must ensure that it draws up, and persons acting on its behalf or on its account draw up, a cryptoasset insider list.*
- 4.12.4 R (1) *A relevant issuer, person responsible for the offer or UK QCATP operator must ensure that the cryptoasset insider list:*
- (a) specifies the date on which the *cryptoasset insider list* was created and updated;
 - (b) is drawn up in accordance with Template 1 of *CRYPTO 4 Annex 1*;
 - (c) is maintained by it or by any *person* acting on its behalf or on its account;
 - (d) is divided into separate sections relating to different *cryptoasset inside information*; and
 - (e) is updated to include new sections to the *cryptoasset insider list* upon the identification of new *cryptoasset inside information*.
- (2) *A relevant issuer, person responsible for the offer or UK QCATP operator:*
- (a) may insert a supplementary section into its *cryptoasset insider list* with the details of individuals who have access at all times to all *cryptoasset inside information* ('permanent cryptoasset insiders'), in accordance with Template 2 of *CRYPTO 4 Annex 1*; and
 - (b) must not include the details of permanent cryptoasset insiders referred to in 2(a) in the sections of the *cryptoasset insider list* referenced in (1).

Maintenance of cryptoasset insider lists

- 4.12.5 R *A relevant issuer, person responsible for the offer or UK QCATP operator must ensure that it or any person acting on its behalf or on its account promptly updates the cryptoasset insider list:*
- (1) when there is a change in the reason why a *person* is on the *cryptoasset insider list*;
 - (2) whenever a new *person* is to be added to the *cryptoasset insider list*; and
 - (3) to indicate the date on which a *person* already on the *cryptoasset insider list* no longer has access to *cryptoasset inside information*.

- 4.12.6 R A *relevant issuer, person responsible for the offer* or UK *QCATP operator* must ensure that every *cryptoasset insider list* prepared by it or by *persons* acting on its account or on its behalf is kept for at least 5 years from the date on which it is drawn up or updated, whichever is the latest.
- 4.12.7 R (1) A *relevant issuer, person responsible for the offer* or UK *QCATP operator* must ensure that it and any *persons* acting on its account or on its behalf draw up and keep the *cryptoasset insider list* up to date in an electronic format in accordance with Template 1 of *CRYPTO 4 Annex 1*.
- (2) Where the *cryptoasset insider list* contains the supplementary section referred to in *CRYPTO 4.12.4R(2)(a)*, a *relevant issuer, person responsible for the offer* or UK *QCATP operator* must ensure that it and any *person* acting on its account or on its behalf draw up and keep that section updated in an electronic format in accordance with Template 2 of *CRYPTO 4 Annex 1*.
- 4.12.8 R The electronic format referred to in *CRYPTO 4.12.7R* must at all times ensure:
- (1) the confidentiality of the information included by ensuring that access to the *cryptoasset insider list* is restricted to clearly identified *persons* who need that access due to the nature of their function or position from within the *relevant issuer, person responsible for the offer* or UK *QCATP operator* or any *person* acting on its behalf or on its account;
- (2) the accuracy of the information contained in the *cryptoasset insider list*; and
- (3) access to, and retrieval of, previous versions of the *cryptoasset insider list*.

Providing cryptoasset insider lists to the FCA on request

- 4.12.9 R (1) Whether the *cryptoasset insider list* is prepared, maintained and/or kept by a *relevant issuer, person responsible for the offer* or UK *QCATP operator* or by *persons* acting on its account or on its behalf, the *relevant issuer, person responsible for the offer* or UK *QCATP operator* must submit the *cryptoasset insider list* to the *FCA* as soon as possible upon request per regulation 31(1)(c) of the *Cryptoassets Regulations* using the means specified by the *FCA* when the *cryptoasset insider list* is requested.
- (2) The means used by a *relevant issuer, person responsible for the offer* or UK *QCATP operator* to submit its *cryptoasset insider list* to the *FCA* must maintain the completeness, integrity and confidentiality of the information during the transmission.

Acknowledgement of legal and regulatory duties

- 4.12.10 R A *relevant issuer, person responsible for the offer* or *UK QCATP operator* must ensure that it or any *person* acting on its behalf or on its account takes all reasonable steps to ensure that any *person* on the *cryptoasset insider list* acknowledges in writing the legal and regulatory duties entailed, and is aware of the sanctions applicable to *cryptoasset insider dealing* and unlawful disclosure of *cryptoasset inside information*.
- 4.12.11 R Where another *person* acting on behalf of or on the account of a *relevant issuer, person responsible for the offer* or *UK QCATP operator* assumes the task of drawing up and updating the *cryptoasset insider list*, the *relevant issuer, person responsible for the offer* or *UK QCATP operator* remains fully responsible for complying with *CRYPTO* 4.12. The *relevant issuer, person responsible for the offer* or *UK QCATP operator* must always retain a right of access to the *cryptoasset insider list*.
- 4.12.12 G Providing *persons* with access to *cryptoasset inside information* and including such *persons* on a *cryptoasset insider list* is without prejudice to the prohibitions laid down in Chapter 2 of the *Cryptoassets Regulations*.
- 4.13 Rules that can be waived or modified
- 4.13.1 G As a result of section 138A of the *Act* (Modification or waiver of rules), the *FCA* has the power to waive all its *rules*, other than *rules* made under section 137O) (Threshold condition code), section 247 (Trust scheme rules), section 248 (Scheme particulars rules), section 261I (Contractual scheme rules) or section 261J (Contractual scheme particulars rules) of the *Act*.

4 Annex Cryptoasset insider list templates

1

4 Annex R

1.1

TEMPLATE 1	
Insider list: section relating to [name of the deal-specific or event-based inside information]	
Date and time (of creation of this section of the cryptoasset insider list – ie, when this inside information was identified):	[yyyy-mm-dd; hh:mm (coordinated universal time (UTC))]
Date and time (last update):	[yyyy-mm-dd, hh:mm (UTC)]
Date of transmission to the Financial Conduct Authority (if applicable):	[yyyy-mm-dd]
First name(s) of the insider	[Text]

Surname(s) of the insider	[Text]
Birth surname(s) of the insider (if different)	[Text]
Professional telephone number(s) (work direct telephone line and work mobile numbers)	[Numbers (no space)]
Issuer/person responsible for the offer/CATP operator name and address	[Address]
Function and reason for being insider	[Text describing role, function and reason for being on this list]
Obtained (the date and time at which a person obtained access to inside information)	[yyyy-mm-dd, hh:mm (UTC)]
Ceased (the date and time at which a person ceased to have access to inside information)	[yyyy-mm-dd, hh:mm (UTC)]
Date of birth	[yyyy-mm-dd]
National identification number (if applicable)	[Number and/or text]
Personal telephone number(s) (home and personal mobile telephone numbers)	[Numbers (no space)]
Personal full home address (street name; street number; city; post/zip code; country)	[Text: detailed personal address of the insider Street name and street number City Post/zip code Country]

4 Annex R
1.2

TEMPLATE 2 Permanent insiders section of the insider list	
Date and time (of creation of the permanent insiders section)	[yyyy-mm-dd, hh:mm (UTC)]
Date and time (last update):	[yyyy-mm-dd, hh:mm (UTC)]
Date of transmission to the Financial Conduct Authority (if applicable):	[yyyy-mm-dd]

First name(s) of the insider	[Text]
Surname(s) of the insider	[Text]
Birth surname(s) of the insider (if different)	[Text]
Professional telephone number(s) (work direct telephone line and work mobile numbers)	[Numbers (no space)]
Issuer/person responsible for the offer/CATP operator name and address	[Address]
Function and reason for being insider	[Text describing role, function and reason for being on this list]
Included (the date and time at which a person was included in the permanent insider section)	[yyyy-mm-dd, hh:mm (UTC)]
Date of birth	[yyyy-mm-dd]
National identification number (if applicable)	[Number and/or text]
Personal telephone number(s) (home and personal mobile telephone numbers)	[Numbers (no space)]
Personal full home address (street name; street number; city; post/zip code; country)	[Text: detailed personal address of the insider Street name and number City Post/zip code Country]