FINANCIAL CONDUCT AUTHORITY

Policy Statement

PS26/11

Crypto Regime

Regulated Cryptoasset Activities

June 2026

This relates to

Consultation Paper CP25/14, CP25/40 and CP26/4 which are available on our website at www.fca.org.uk/publications

Email:
cp26-4@fca.org.uk

All our publications are available to download from www.fca.org.uk.

Request an alternative format

Please complete this form if you require this content in an alternative format.

Or call 0207 066 1000

Sign up for our **news and publications alerts**

See all our latest press releases, consultations and speeches.

Contents

Chapter 1

Summary

1.1 In this Policy Statement, we set out our final rules and guidance for the regulated cryptoasset activities defined by the Regulated Activities Order, including operating a qualifying cryptoasset trading platform (QCATP), dealing, arranging, lending and borrowing, staking, safeguarding and our current approach to decentralised finance (DeFi). The framework is intended to provide a clear and proportionate conduct baseline for core cryptoasset business models.

1.2 Consultation feedback was broadly supportive, although respondents raised concerns in a number of areas, including pre-trade transparency requirements for principal dealers, UK execution venue requirements, the application of best execution, the breadth of the arranging perimeter, and the treatment of DeFi interfaces and international firms. Respondents also sought greater clarity in certain areas, in particular best execution and the position of international firms.

1.3 In light of feedback, we have retained the overall framework, while making targeted amendments and providing further guidance. In particular, principal dealers have been removed from pre-trade transparency requirements, in line with the updated approach in non-equity traditional finance. We have also clarified expectations on best execution, including that firms should check prices from at least three reliable UK authorised execution venues where possible, but are not required to execute on those venues or undertake mechanical transaction-by-transaction checks, provided they maintain effective overall arrangements supported by periodic post-trade analysis. Beyond UK QCATPs and intermediaries, this Policy Statement confirms retail protections for cryptoasset lending, borrowing and staking, targeted refinements to collateral and auto-staking rules, and the application of safeguarding requirements under CASS 17 with adjustments to reflect cryptoasset custody. For Decentralised Finance (DeFi), we intend to proceed on the basis that rules apply where there is an identifiable controlling entity, with separate guidance to follow on how decentralisation will be assessed in practice. DeFi is an industry term used to market a range of financial services with a high degree of automation.

1.4 This Policy Statement should be read in conjunction with other FCA publications. For example, PS26/9 contains the admissions, disclosures and market abuse framework, and PS26/12 sets out the prudential requirements for cryptoasset firms. In addition, PS26/13 sets out how additional cross cutting Handbook requirements apply to cryptoasset firms, including areas such as Consumer Duty, COBS, SM&CR, regulatory reporting, safeguarding and Approach to International Cryptoasset Firm guidance.

1.5 In each chapter, we summarise the feedback to our proposals which we consulted on in CP25/14, CP25/40 and CP26/4 and explain our response as reflected in the final rules and guidance for each activity.

Chapter 2

Cryptoasset Trading Platforms

2.1 This chapter focuses on the activity of operating a qualifying cryptoasset trading platform (QCATP) which was discussed in Chapter 2 of CP25/40 and in the draft guidance to our wider Approach to International Cryptoasset Firms in Annex 4 of CP26/4.

Overview of CP25/40 Consultation Proposals

2.2 In CP25/40, we consulted on the following proposals:

Section/topic	Question(s) in CP25/40
Location, incorporation, and authorisation of UK QCATPs	Question 1
Platform access and operation requirements	Question 2
Retail customer focused requirements	Question 3
Rules to manage specific conflicts of interest and related risks	Question 4
Transparency, record keeping and reporting requirements	Questions 17-19
Settlement arrangements	Question 5

Location, incorporation, and authorisation of UK QCATPs

Consultation proposals

2.3 The Cryptoassets Regulations require firms to obtain FCA authorisation as a UK QCATP operator if they operate a QCATP in the UK or, where the platform is serving UK consumers, from overseas.

2.4 We proposed in CP25/40 that firms seeking UK authorisation should have a UK presence. We also proposed that, where it would enable access to global liquidity, there are circumstances in which a UK QCATP operator could combine a UK legal entity with UK authorisation of an overseas QCATP via a UK branch. We also indicated that separate guidance would be consulted on to clarify our general expectations for international cryptoasset firms seeking FCA authorisation. This consultation was part of CP26/4 (see Annex 4).

2.5 In CP25/40, we asked:

Question 1: **Do you agree with our proposals on location, incorporation and authorisation of UK CATPs? If not, please explain why not?**

Feedback

2.6 There were 42 respondents to this question. 95% of these respondents supported or were neutral to our proposals.

2.7 Respondents who were supportive of our proposals agreed with our objectives to provide protections to UK consumers while allowing flexibility on the legal form of a firm's UK presence where it would facilitate UK consumer access to global liquidity.

2.8 However, 7 of these responses pointed to potential liquidity fragmentation and increased operational costs stemming from a requirement to have a separate UK order book.

2.9 Six of these responses requested further guidance on potential business models permitted within the proposed subsidiary and branch combined structure, and the permitted allocation of activities between the subsidiary and the branch, where this model was deemed appropriate. Respondents also noted that they would consider and respond to subsequent consultation paper CP26/4 which provided further guidance on our proposed Approach to International Cryptoasset Firms (AICF). A summary of the feedback to that consultation, and our response and finalised guidance can be found in PS26/13. Our finalised guidance can be found in FG26/7.

2.10 Some responses raised concerns about the cross-border aspect of our proposals. They cited substance-over-form risk, potential information sharing difficulties, insolvency risks and potential enforcement difficulties. Suggestions were made that included ensuring, as part of the authorisation process, that UK QCATPs are subject to a 'substance test' to make sure they have effective UK governance and controls.

2.11 Two respondents were unsupportive of our proposals. One response cited the risk of an asymmetric market where the perimeter requires authorisation for overseas firms serving UK consumers and does not for firms serving only institutional clients. The second response cited the need for guidance on how the perimeter applies to firms undertaking DeFi activities.

Our response

We have carefully considered the feedback, and we have proceeded with our proposals as consulted on.

In answer to the feedback setting out the risk of an asymmetric market arising from the perimeter, which requires authorisation for overseas firms serving UK consumers while not requiring this for firms serving institutional clients, these requirements stem from the perimeter set out in the Cryptoassets Regulations and are further explained in the cryptoasset perimeter guidance that we consulted on in CP26/13. The approach in the Cryptoassets Regulations seeks to make sure that persons offering certain services to UK consumers are within scope of the perimeter, regardless of whether they are based in the UK or overseas.

For overseas QCATP operators offering services to UK consumers, our final AICF guidance sets out that in certain circumstances, firms can combine a UK legal entity presence with UK authorisation of an overseas-incorporated QCATP operator via a UK branch. Whether such a set-up meets our threshold conditions for authorisation of the overseas-incorporated QCATP operator will be assessed on a case-by-case basis at the FCA authorisation gateway. Similarly, any subsequent structural changes will be considered on a case-by-case basis in supervision. This enables, in certain circumstances, firms to offer direct access to global liquidity pools on overseas QCATPs while providing consumer protections and allowing appropriate regulatory oversight.

From the feedback, it appears that parts of our proposals may have been misunderstood. To clarify the feedback described in paragraph 2.8, we do not require a separate UK order book where an overseas QCATP operator is authorised in the UK via a branch. Authorisation via a branch of the overseas QCATP operator requires a whole-firm assessment and brings the regulated activities of the entire overseas entity into scope of UK regulation, including the threshold conditions and applicable Handbook requirements.

Having considered the feedback, we are not issuing more prescriptive guidance on potential business models that would be permitted under the proposed subsidiary and branch combined structure nor on the permitted allocation of activities between the subsidiary and the branch. This is because queries about specific arrangements by QCATP operators seeking authorisation via a UK branch can be assessed on a case-by-case basis rather than through non-Handbook guidance. Firms should consider the outcomes set out in the final legal instrument and in our AICF guidance and propose a solution which works for their business model. This will be assessed case-by-case at the authorisation gateway.

Where a firm seeks UK authorisation for an overseas QCATP via a UK branch, it will need to demonstrate why authorisation as a branch is appropriate for its business model and carefully assess the scope of UK regulatory requirements. For example, some rules, such as threshold conditions for authorisation and prudential requirements, will apply to the legal entity operating the platform, while others may apply only to the activity of operating a QCATP or to the operation of the specific platform that triggers the authorisation requirement. Firms should refer to individual sourcebooks, our Approach to International Cryptoasset Firms (AICF) guidance (see FG26/7) and our existing Approach to International Firms (AIF) guidance for further detail.

Our responses on feedback relating to DeFi can be found in Chapter 9: Decentralised Finance (DeFi).

Having carefully considered the feedback to CP26/4 regarding the scope of COBS and DISP for users of an overseas QCATP authorised in the UK via a branch, we have limited the application of both COBS and DISP to UK-based users of these branch-authorised QCATPs. However, we refer readers to PS26/13 Chapters 10 (COBS) and 12 (DISP) and the AICF for further detail on certain limitations on the application scope of certain existing Handbook rules in relation to overseas QCATP operators authorised in the UK via a branch.

Platform access and operation requirements

Consultation proposals

2.12 In DP25/1 we proposed requirements for fair, non-discriminatory platform access and operation and orderly markets. In CP25/40, we consulted on these proposals, with some adjustments to reflect feedback.

2.13 In relation to algorithmic and automated trading, we consulted on a principles-based approach. This requires UK QCATP operators to set out rules for the types and uses of algorithms, monitor algorithmic trading activity and disclose information related to algorithmic trading on the platform.

2.14 We have also provided more detail on obligations relating to market-making arrangements, including confirming that we will not require formal contracts in place with all market-makers. However, where a UK QCATP offers incentive schemes or has any other legal, contractual, or commercial arrangement with market makers or other liquidity providers, the UK QCATP operator must document and disclose such schemes and relationships, including their terms. The operator also must identify, document and monitor users who carry out market making strategies on its UK QCATP.

2.15 In addition, we signposted key operational obligations under the Market Abuse Regime for Cryptoassets (MARC) for UK QCATP operators. These included on-chain monitoring requirements for large UK QCATP operators, maintaining appropriate information barriers and insider lists, and establishing and maintaining effective systems and controls to prevent, detect and disrupt market abuse on their platform.

2.16 In CP25/40 we asked:

Question 2: **Do you agree with our proposals on UK QCATP access and operation requirements? If not, please explain why not?**

Feedback

2.17 There were 41 respondents to this question. 71% of these respondents were supportive of our proposals. Of these responses, 27% (8 respondents) provided suggestions or queries.

2.18 Respondents agreed that UK QCATPs should be neutral trading venues. They also agreed that fair and orderly trading services along with clear disclosures and robust systems and controls would improve UK consumer confidence in cryptoasset markets.

2.19 Respondents agreed with our proposals for mitigating the risks that poor market making and use of trading algorithms can pose to orderly markets. Respondents felt that the proposed reliance on a principles-based approach was well-suited to cryptoasset markets and would support liquidity and competition. They also supported the flexibility the proposals would allow across different UK QCATP models.

2.20 While supportive of our proposals, respondents requested further guidance on requirements involving algorithmic trading activity, including worked examples on algorithmic controls, minimum testing requirements and the extent of kill switch capabilities.

2.21 Some responses suggested that UK QCATPs should carry out on-chain monitoring for market abuse regardless of their size. This and other feedback on the MARC regime is addressed in PS26/9.

2.22 One firm suggested that our UK QCATP-specific operational resilience related requirements were too prescriptive, while another felt that our requirements to prevent disorderly markets were too inflexible. (Broader feedback on general operational resilience requirements in the SYSC sourcebooks and our response to that feedback can be found in PS26/13.)

2.23 Among the unsupportive responses (7%) opinions were split, with opposing views on our algorithmic trading requirements. Two responses argued that our proposals were too burdensome for new entrants. The third response argued that these proposals were not prescriptive enough, suggesting requirements should reflect MiFID RTS 6 rules applicable to Multilateral Trading Facilities.

Our response

Having considered the feedback carefully, we have proceeded with our proposals to require UK QCATP operators to define and implement non-discriminatory rules and procedures for platform access and operation, including objective criteria for platform access and non-discretionary rules for order execution. We believe these rules will support market integrity, help to protect consumers and improve consumer confidence in UK cryptoasset markets.

Our final rules set out that UK QCATP operators must ensure that their systems, procedures, controls and arrangements for operation of the UK QCATP are adequate, effective and commensurate to the size and nature of the business carried out on the platform. This includes our CRYPTO 6 UK QCATP-specific operational resilience related requirements and our requirements on measures to prevent disorderly markets for UK QCATP operators as consulted on. We believe these rules, which align in principle with those required for MTFs under MAR 5, can be applied to UK QCATPs regardless of size or business model and do not require more flexibility. In sum, we believe these requirements will ensure that firms are able to reduce the likelihood of things going wrong and reduce the risk of contagion should something go wrong. We expect this will help to ensure orderly markets and protect consumers. Further systems and controls requirements and the scope of their application are discussed in more detail in PS26/13 under SYSC and AICF Chapters.

We set out in our final rules, as consulted on, UK QCATP operators' obligations in relation to market-makers and algorithmic trading on a UK QCATP, to support fair and orderly trading for UK markets and investors. We maintain our principles-based approach to regulating algorithmic trading in the final rules. We continue to believe that this strikes the right balance between mitigating against the potential risk to orderly markets and reflecting the still nascent and fast-evolving nature of cryptoasset markets. We will monitor the operation of these rules and make changes in the future should the market evolve to warrant them.

Regarding the general requests for further guidance on algorithmic trading controls, we are not providing additional guidance in our final rules. This is because these rules are outcomes-based and intended to give firms the flexibility to allow use of both small and large-scale algorithms as is right for their business. Our principles-based approach recognises the early-stage development of the industry compared to traditional finance (TradFi). However, we will continue monitoring the use and control of algorithms as they evolve.

In relation to the feedback on the extent of kill switch capabilities, our rules are intended to protect UK users of a UK QCATP and so they should not be read as requiring a kill switch to extend across global activity. For instance, firms could potentially make use of local user access controls (or other measures) to halt use within a particular region should the circumstances for their use arise.

Retail customer focused requirements

Consultation proposals

2.24 In CP25/40, we proposed additional protections for UK retail users of UK QCATPs. This was because direct retail access to QCATPs is possible in cryptoasset markets. This is different from the generally intermediated access to Multilateral Trading Facilities (MTFs) in TradFi. The proposals we consulted on included restrictions linked to the Admissions and Disclosures (A&D) regime (see PS26/9 for detail), where we proposed that UK retail investors must only be given access to qualifying cryptoassets if the asset is a UK-issued qualifying stablecoin or is admitted to trading on a UK QCATP with a qualifying cryptoasset disclosure document (QCDD). Certain related notification and disclosure requirements must be met too.

2.25 We also set out expectations around providing clear and timely information for all users on terms, fees, trading rules, settlement arrangements and conflicts of interest.

2.26 In addition, the application of Consumer Duty obligations to the activity of operating a UK QCATP was discussed in CP26/4. Feedback on CP26/4 and finalised guidance are discussed in PS26/13.

2.27 In CP25/40 we asked:

Question 3: **Do you agree with [the above] proposals on additional rules to protect UK retail customers? If not, please explain why not?**

Feedback

2.28 There were 42 respondents to this question. 74% of these respondents were supportive of our proposals. Responses supported our proposals to ensure UK retail consumers are well informed and appropriately protected.

2.29 Four responses asked for deferral arrangements to allow firms the necessary time to prepare relevant QCDDs for tokens already in circulation and requested clarity on the application of the Consumer Duty and its interaction with QCDDs.

2.30 Where respondents were unsupportive of our proposals (7%), they requested that UK authorised intermediaries should also have the power to make qualifying cryptoassets accessible to UK retail customers, and argued that restricting UK retail access by requiring admission to trading on UK QCATP would delay UK retail consumer access to new projects and may push these users offshore where they may have fewer consumer protections. A further respondent raised concerns regarding a scenario where there may be no identifiable issuer.

Our response

We have proceeded with our retail customer focused requirements for UK QCATPs as consulted on. These rules work alongside the A&D regime and provide additional protection for UK retail customers. So, UK QCATP operators, regardless of where they are based, must:

- Make sure that UK retail investors can only access qualifying cryptoassets on the operator's platform that have been admitted to trading for retail investors, with an A&D-compliant QCDD (unless the product is a UK-issued qualifying stablecoin).
- Direct UK retail customers to the relevant QCDD(s) (and, where applicable, Supplementary Disclosure Document(s) (SDD(s)) before an order is placed. Where there are two or more relevant QCDDs (eg, because tokens on different chains are considered interchangeable by a QCATP when traded on or deposited to that QCATP), the firm must direct all users to all relevant QCDDs (and SDDs, where relevant).

Further, UK QCATP operators will need to make sure that for all users:

- Arrangements are in place to ensure that notification and disclosure obligations are met in case a qualifying cryptoasset is withdrawn from (and so no longer admitted to) trading.
- Clear and timely disclosures on terms, fees, trading rules, settlement arrangements and conflicts of interest are provided.

For all users, firms need to ensure that this information is appropriately accessible. Where related to consumers, these disclosures are subject to obligations under the Consumer Duty.

In relation to feedback requesting that UK authorised intermediaries should also have the power to make qualifying cryptoassets available to UK retail customers, under our rules this is broadly reserved for UK QCATP operators as only they can admit tokens with QCDDs onto a UK QCATP.

We refer readers to PS26/9 for responses and feedback relating to identification of issuers under the A&D regime.

We have noted the requests for deferral arrangements for the preparation and publication of QCDDs. We intend to consult in September 2026 on creating an optional deferral mechanism. This is likely to include extending by six months the time for UK QCATP operators to admit to trading, with an A&D-compliant QCDD, any qualifying cryptoassets traded on their platform by retail investors (ahead of go-live in October 2027). Work is still ongoing on this deferral proposal, so it remains subject to change.

Feedback on the proposed scope of the Consumer Duty and final guidance on its application to UK QCATPs are discussed in PS26/13. Readers may also wish to refer to the Mansion House response letter from September 2025 for a broader perspective on the direction of travel on the Consumer Duty.

Rules to manage specific conflicts of interest and related risks

Consultation proposals

2.31 We proposed rules to address UK QCATP-specific conflicts of interest and financial risks.

2.32 Taking into account feedback to our DP25/1 and DP24/4, we consulted on proposals to:

- Allow UK QCATP operators to engage in matched principal trading (MPT) subject to a number of conditions – in line with recent changes in the equivalent TradFi rules for MTFs.
- Allow firms to run a (non-matched) principal dealing desk in the same legal entity that operates the QCATP, subject to a number of conditions, including that the principal dealing desk must not access the QCATP in the same entity to execute trades.
- Permit affiliates of a UK QCATP operator to access the UK QCATP, subject to conflict mitigation.
- Allow issuance/admission of tokens where a UK QCATP operator has a financial interest, also subject to sufficient conflicts mitigation/management.

2.33 We also consulted on proposals to require legal separation where credit risk exposure (other than settlement risk) arises.

2.34 Additionally, we proposed to apply personal account dealing rules similar to those under COBS 11.7 to UK QCATP operators.

2.35 In CP25/40 we asked:

Question 4: **Do you agree with our proposals to manage conflicts of interest and related risks? If not, please explain why not?**

Feedback

2.36 There were 43 respondents to this question. 80% of these respondents were generally supportive of our revised proposals. Respondents agreed that effective conflict mitigation could be achieved through strong controls, governance and oversight.

2.37 However, of the supportive respondents to Question 4:

- Three suggested additional requirements to ensure that preferential access is not given where an affiliate is able to trade on the UK QCATP.
- Three raised concerns or suggestions about our proposals to allow UK QCATPs to issue tokens in which they have a financial interest. One suggestion was to restrict this to only UK-issued qualifying stablecoins to limit price volatility. Others argued that allowing a UK QCATP to issue a token in which it has a financial interest would be a material departure from established market structure principles, particularly where CATPs and MTFs compete for the same liquidity.

- Four requested further guidance on which conflict-of-interest mitigants would be considered sufficient, with 1 saying that this would allow firms to combine these 'approved mitigants' proportionately, depending on their business model.

2.38 Four respondents were not supportive of our proposals to allow matched principal dealing within the same legal entity that operates a UK QCATP. They found our proposed mitigants insufficient to address conflicts that could arise, particularly where that QCATP serves retail clients. One respondent highlighted the need for suitability assessments and the Consumer Duty requirements. A second respondent suggested this would differ from rules applicable to MTFs in TradFi.

Our response

We have proceeded with our proposals to allow a firm to act as a matched principal dealer provided it complies with the relevant conditions and rules. This is to align with recent changes of rules for MTFs as set out in PS25/17. We do not consider it proportionate at this time to have stricter requirements for crypto firms than for firms in TradFi. Protections remain in place for retail customers using this service through the additional requirements for UK QCATP operators, including regarding access only to tokens admitted to trading on the platform with an A&D-compliant QCDD. See Our response (paragraph 2.30) above for more on our retail customer focused requirements.

We refer respondents who requested suitability assessments and the Consumer Duty to our respective COBS and Consumer Duty chapters in PS26/13, where we discuss these in more detail.

We have also proceeded with our proposals to permit own tokens, including those in which the operator has a financial interest, to be admitted on a UK QCATP. We believe that combined with A&D-specific requirements on both conflicts of interest and for firms admitting a token in which they have a financial interest (see final rules in CRYPTO 3.2.8R – 3.2.9R and 3.4.6R respectively), and SYSC 10 requirements on conflicts of interest, our requirements for QCATP operators to have in place sufficient policies and procedures to mitigate the risk from this conflict of interest provide sufficient protections for customers.

We have also proceeded with our proposals to allow affiliates of a UK QCATP operator to trade on the platform. We believe that our CRYPTO 6 rules on non-discriminatory access to UK QCATPs and co-location will ensure that preferential access is not given to any affiliate trading on the platform.

We have not provided any additional guidance on what constitutes sufficient conflict of interest mitigants. This is because we believe it is for firms to determine the specific conflicts of interest that are related to their business models and size and how best to mitigate these. We encourage firms to refer to the examples of conflicts and reasonable mitigants listed in paragraph 2.24 of CP25/36 on Client categorisation and conflicts of interest for more colour.

We have proceeded with the other proposals set out in paragraphs 2.32 to 2.34 above. We believe that conflict of interest mitigants (including the prohibition for principal dealers to deal on their own platform) are at least equally effective and more proportionate and targeted than requiring legal entity separation for principal dealers or banning trading by affiliates.

Regarding our rules on credit risk exposure, we believe that QCATP operators should be risk-neutral venues and exposure to credit risk within the same entity may undermine platform stability.

On our personal account dealing rules, we believe that these are an important element to mitigate conflicts that could arise between employees of a firm on the one hand and the firm's clients or the firm itself on the other.

Settlement arrangements

Consultation proposals

2.39 In CP25/40, we outlined a high-level settlement approach where firms would have flexibility over whether they internalise settlement or arrange it externally, provided they ensure clients understand the firm's settlement responsibilities. We also indicated that a fuller set of settlement requirements and related guidance would be consulted on later, in CP26/4 and the perimeter guidance for the new regulatory regime.

2.40 Both have since been published. CP26/4 explained in the CASS Chapter (Chapter 9) and in the AICF (Annex 4) that UK QCATPs may operate a settlement 'float', subject to certain conditions and limitations.

2.41 Article 9Q of the Cryptoassets Regulations provides for a temporary settlement exclusion from the perimeter of the safeguarding activity. Our cryptoasset perimeter guidance consultation in CP26/13 sets out our proposed expectations for firms seeking to rely on this exclusion (see PERG19.6.6 and 19.6.7).

2.42 In CP25/40, we asked:

Question 5: **Do you agree with our high-level proposals on settlement? If not, please explain why not?**

Feedback

2.43 76% of respondents were supportive of our proposals. 24% were neutral or unclear in their view, with some pointing to further feedback they planned to provide to CP26/4.

2.44 Respondents who were supportive and those who were unclear/neutral requested guidance on settlement timings and how these obligations interact with custody and reconciliation duties.

Our response

We have proceeded with our proposals to allow firms flexibility over whether they internalise settlement or arrange it externally. The final rules provide for firms to be able to settle transactions off-chain where it may be more cost-effective and hence enable better execution outcomes for clients.

Regarding requests for guidance on settlement timings, CRYPTO 6 guidance clarifies that we expect settlement to be initiated within 24 hours of a trade being executed.

Details of our final rules in relation to operating a QCATP settlement 'float' have been set out in Chapter 7: Safeguarding of this PS and the final AICF can be found in PS26/13.

Final perimeter guidance, including expectations in relation to the use of the temporary settlement exclusion from Safeguarding, will be published in due course.

Chapter 3

Cryptoasset Intermediaries

3.1 This chapter describes the feedback we received on our proposals for cryptoasset intermediaries set out in Chapter 3 of CP25/40. It also sets out our response.

3.2 'Cryptoasset intermediaries' refers to persons performing any of the following activities defined by the Treasury in the Cryptoassets Regulations:

- Dealing in qualifying cryptoassets as principal;
- Dealing in qualifying cryptoassets as agent; and
- Arranging deals in qualifying cryptoassets.

Overview of CP25/40 consultation proposals

3.3 In CP25/40, we consulted on the following proposals:

Section/topic	Question(s) in CP25/40
General execution and dealing rules	Questions 6–10
Specific eligibility and execution requirements for retail orders	Questions 11–12
Rules to manage specific conflicts of interest	Questions 13–15
Transparency, record keeping and reporting requirements for intermediaries	Questions 17–19
Settlement	Question 16

General execution and dealing rules

Consultation proposals

3.4 We proposed to apply best execution obligations and client order handling rules in a way that is aligned with the TradFi approach. Further, we consulted on draft guidance covering checking reliable price sources from UK-authorised execution venues. This guidance clarified our expectations around over-reliance on a single, often affiliated execution venue or internal pricing methodologies, and highlighted the importance of surveying available prices on the market.

3.5 We consulted on the application scope of the proposed rules, the role of client instructions and total consideration, and disclosure to clients. We also proposed cryptoasset-specific pre-trade disclosures by principal dealers.

Question 6 – further guidance on best execution

Consultation proposals

3.6 We provided detailed discussions of the proposed best execution framework in CP25/40, including the application scope of the proposed best execution rules, the role of client instructions and total consideration.

3.7 In CP25/40 we asked:

Question 6: **Is any further guidance on best execution required? If so, what additional guidance can we provide to clarify the scope of and expectations around best execution?**

Feedback

3.8 There were 25 responses to this question. 96% of these responses were supportive of further implementation guidance on best execution, with the remaining 4% being neutral. These respondents called for further guidance that focuses on whether firms are achieving the desired execution outcomes in practice, and have appropriate execution policies supported by data, governance, and monitoring.

3.9 Respondents shared a general view that best execution should not be judged as a trade-by-trade mechanical benchmark, but rather as a framework that is assessed over time. They preferred more practical and crypto-specific guidance as opposed to rigid tests or high-level principles. They also sought further guidance on how firms should weigh and document other execution factors beyond price, such as certainty of execution, speed, settlement timeliness, and venue reliability.

3.10 Respondents were also interested in further guidance on how to evidence compliance, for example what monitoring and testing should look like and how to document venue selection processes.

3.11 A minority of respondents also argued that the FCA should clarify the application of the proposed rules to certain principal dealing models, for example matched principal dealing and hedging.

3.12 There was a strong call for deferral arrangements or phased implementation of the proposed best execution rules. Some were worried that liquidity is too fragmented for the immediate implementation of the proposed best execution requirements. Under the proposed regime, most notably the execution venue requirement, respondents said intermediaries would not have a realistic ability to diversify liquidity sources on day one. This is especially relevant where UK QCATPs may not yet be fully operational, authorised, or able to offer meaningful depth of liquidity immediately at regime go-live. So, deferral arrangements were seen as important in providing flexibility to firms and facilitating their compliance with the best execution obligations.

Our response

We have proceeded with the proposed best execution rules. This means when executing orders, a firm must take sufficient steps to obtain the best possible results for its clients, taking into account the execution factors such as price, costs, and speed.

The best execution rules create a consistent set of standards for firms, helping them to deliver improved execution outcomes for clients and to protect clients' best interests. Such rules are particularly important as part of cryptoasset regulation, given opaque market practices and fragmented liquidity pools that currently exist in this market.

In line with the general understanding of respondents, we confirm that the final rules and guidance for cryptoasset best execution rules do not impose mechanical, transaction-by-transaction checks. Best execution is essential to ensuring a high standard of conduct by delivering good client outcomes. Instead of a tick-box process, firms are required to implement effective overarching best execution arrangements, taking into account transaction- and business-model-specific factors. At a minimum, we expect firms to have in place adequate, periodic post-trade analyses to evidence compliance.

Our final rules and guidance clarify that the proposed best execution rules do not apply to UK QCATP operators conducting matched principal trading on their own platform. This reflects the nature of this particular business model and the conditions it is subject to, as the transactions are executed on the UK QCATP and in accordance with the non-discretionary rules of it.

We consider these additional clarifications to be sufficient without being overly prescriptive at this stage. We expect market practices to evolve, including as a result of the new regime. As a result, we will continue to monitor this area and consider targeted clarification through supervisory publications and communications if and when needed.

We have noted the requests for deferral arrangements and intend to consult on creating a deferral mechanism with respect to execution policies, extending by 3 months to January 2028, the time when intermediaries must have received consent to their updated execution policy. We intend to consult on this in September of this year.

Question 7 – guidance to check 3 price sources from UK-authorised execution venues

Consultation proposals

3.13 We proposed guidance that where firms need to comply with best execution obligations, they should check at least 3 reliable price sources from UK-authorised execution venues (if available). If fewer than 3 UK-authorised execution venues can execute the order, firms should check the available UK ones.

3.14 In CP25/40 we asked:

Question 7: **Do you agree with our proposed guidance (including the exemptions proposed) to check at least 3 reliable price sources from UK-authorised execution venues, such as a CATP or principal dealer (if available)? If not, please explain why not?**

Feedback

3.15 There were 38 responses to this question. 61% of responses were unsupportive of our proposed guidance to check at least 3 reliable price sources from UK-authorised execution venues.

3.16 Several unsupportive respondents called for clarification that the guidance on checking prices does not introduce further restrictions on liquidity sourcing. They argued, for instance, that the guidance should not impede a principal dealer hedging its own positions on offshore execution venues.

3.17 The feedback also indicated that firms would benefit from specific explanation of what constitutes 'checking prices'. For example, some sought clarification that firms are not required to execute only on the 3 platforms checked under this guidance, and can instead execute orders on other execution venues if doing so delivers better execution outcomes and is otherwise permitted by our rules.

Our response

We have proceeded in our final rules and guidance with the proposed guidance to check at least 3 reliable price sources from UK-authorised execution venues (if available). We expect this guidance to help firms create well-formulated order execution policies (although firms are not required to include the execution venues that it checks prices on in their execution policies) that can be assessed by the firms, their clients and us over time and to support more consistent and effective implementation of best execution across firms.

As a result, where firms are subject to best execution obligations, we expect them to check at least 3 reliable price sources from UK-authorised execution venues (if available), for example to guide the formulation of any price benchmarks they use. If there are UK QCATPs making prices publicly available, we expect firms to prioritise checking these on-platform prices. If fewer than 3 UK-authorised execution venues can execute the order, firms should check these UK-authorised execution venues.

This guidance does not replace the general best execution expectations and is not intended to be a per-transaction mechanical test against prescribed benchmarks.

In the feedback there were several misunderstandings, including where respondents incorrectly conflated sourcing liquidity with checking prices. To address this and other misunderstandings and concerns of respondents, in our final rules and guidance we have further clarified that the guidance is not intended to:

- require a firm to execute a client order on the UK-authorised execution venues it has checked;
- require a firm to include the UK-authorised execution venues that it checks prices on in its execution policy; or
- prevent a firm from additionally considering prices on non-UK qualifying cryptoasset execution venues provided that these venues meet the equivalent standards of governance, operational integrity and market abuse controls.

However, we expect firms to be able to demonstrate that their best execution policy delivers outcomes that are at least as good as execution on those UK-authorised execution venues where prices are checked, for comparable orders.

Question 8 – general disclosure requirements

Consultation proposals

3.18 We proposed general disclosure requirements for cryptoasset intermediaries, including that firms must clearly and prominently disclose their role(s) to retail or professional clients before executing their orders.

3.19 In CP25/40 we asked:

Question 8: **Regarding the general disclosure requirements when firms serve retail or professional clients, what changes or additions may help client understanding?**

Feedback

3.20 We received 24 responses to this question. 63% of respondents were supportive of the proposed general disclosure requirements, and a further 33% were neutral. Responses broadly supported the view that clients need to understand a firm's role in a transaction. This includes, for example, being clear about whether the firm acts as principal, agent, or some combination of roles, and whether the client is trading directly with the firm or the firm is executing on behalf of the client.

3.21 Most respondents supported the suggestion that client understanding would be improved by better and more targeted disclosure. Feedback also went into considerable detail on how disclosure can be improved in practice, for example via layered disclosures including a short summary and optional drilldowns, and appropriate timing of disclosures in the consumer journey.

3.22 Several responses also cautioned against duplication of disclosures and reliance on long, 'boilerplate' terms and conditions.

Our response

Having carefully considered all the feedback, we have proceeded with our proposed disclosure requirements as consulted on. This means in-scope firms must clearly and prominently disclose their role(s) to retail or professional clients before executing client orders. This includes disclosing whether the firm will act as a principal or agent for each order.

Where a firm's order execution policy provides for the possibility that client orders may be executed outside a UK QCATP, a firm must, in particular, inform its retail or professional clients about that possibility. It must also obtain express prior client consent before proceeding to execute their orders outside a UK QCATP.

We also refer readers considering these disclosure requirements to other disclosure rules in this Policy Statement that apply to intermediary firms. Firms must also consider our expectations under the Consumer Duty where relevant.

Question 9 – specific pre-trade disclosure requirements

Consultation proposals

3.23 We proposed that intermediaries dealing as principal and serving retail or professional clients should make appropriate pre-trade disclosures to them, and we specified the disclosures that are required.

3.24 In CP25/40 we asked:

Question 9: **Do you agree with the proposed specific pre-trade disclosures to clients by principal dealers? If not, please explain why not? Do you have any suggestions that can make these disclosures more effective?**

Feedback

3.25 There were 24 responses to this question. Over 90% of these were supportive of our proposed specific pre-trade disclosures by principal dealers. Respondents generally considered these disclosures to promote informed decision-making, fair pricing, and execution transparency. They said clear and easy-to-understand disclosures contribute to stronger consumer protection, particularly for retail clients.

3.26 Some responses also pointed out that the requirements should be clearly targeted at genuine principal dealing, while certain matched principal models may need different treatment.

Our response

We have proceeded with the proposed disclosure requirements as consulted on. This means a firm in scope must disclose to its client prior to execution of the client's order information including:

1. A firm price at which the order can be executed.
2. The duration of the time period for which the firm can execute the order at that price.
3. Any fees or charges for the execution of the order.

When a firm engages in matched principal trading for the purpose of executing client orders on a UK QCATP it operates, and acts in accordance with the non-discretionary rules of the UK QCATP, the firm does not decide a quoted price on its own. We are thus of the view that the nature of this business model means (1) and (2) above, and the related requirements, do not apply.

We also refer readers considering these disclosure requirements to other disclosure rules in this Policy Statement that apply to intermediary firms. Firms must also consider our expectations under the Consumer Duty where relevant.

Question 10 – client order handling rules

Consultation proposals

3.27 We proposed that firms should implement procedures and arrangements which provide for the prompt, fair and expeditious execution of client orders, relative to other orders or the trading interests of the firm.

3.28 In CP25/40 we asked:

Question 10: **Do you agree with the proposed client order handling rules? If not, please explain why not?**

Feedback

3.29 We received 23 responses to this question, and all were supportive of the proposed client order handling rules. They supported that such rules reflect established principles of prompt, fair, and orderly handling of client orders and provide a clear framework for managing conflicts between client orders and a firm's own trading interests.

3.30 Several respondents also welcomed the decision to mirror the approach taken in TradFi, which promotes consistency with established regulatory practice.

3.31 Respondents emphasised that implementation of these rules must accommodate the technical and operational features of crypto markets.

Our response

We have introduced the client order handling rules as consulted on. Having these rules in place helps mitigate risks of significant client harm that may arise during the order execution process.

This means firms in scope must implement procedures and arrangements which provide for the prompt, fair and expeditious execution of client orders, relative to other orders or the trading interests of the firm.

With respect to respondents' comments on implementation, we have already proposed guidance in CP25/40 to assist firms in complying with these requirements. For example, we provided guidance that orders should not be treated as otherwise comparable if they are received by different media and it would not be practicable for them to be treated sequentially (CRYPTO 5.6.3G). We consider such guidance to be sufficient.

Specific eligibility and execution requirements for retail orders

Consultation proposals

3.32 In CP25/40, we proposed an execution venue requirement under which orders for UK retail or elective professional clients should be executed only on UK-authorised execution venues. We also proposed an admission to trading requirement for cryptoassets bought or sold by UK retail clients and support for such clients where admission is subsequently withdrawn.

Question 11 – execution venue rules for UK retail/elective professionals

Consultation proposals

3.33 We proposed to require cryptoasset intermediaries that are executing, or receiving and transmitting orders for UK retail or elective professional clients to ensure these orders are ultimately executed only on UK-authorised execution venues. We also proposed restrictions on where a firm that is affiliated with a QCATP operator can systematically or predominantly source liquidity from when executing orders for UK retail or elective professional clients as a principal.

3.34 In CP25/40 we asked:

Question 11: **Given the overall location policy established by the amendments to section 418 of FSMA and set out in the Cryptoassets Regulations, do you agree with our proposed execution venue requirement? If not, please explain why not? What changes do you propose?**

Feedback

3.35 This question received 34 responses. Feedback on our proposed execution venue requirement was split with 41% being supportive of the proposal and 47% expressing concerns (with the remaining 12% being neutral).

3.36 Those who were supportive of our proposal argued that this rule can reduce the risk that UK retail clients are exposed to poorly governed overseas execution venues or markets with weaker transparency or surveillance. They considered it imperative that UK retail clients transact in cryptoassets within a framework subject to appropriate FCA authorisation, supervision and enforcement. The proposed restriction on systematically or predominantly sourcing liquidity from affiliated overseas QCATPs, they argued, creates a level playing field between firms that incur the cost of becoming UK-authorised, and unauthorised QCATP operators that could otherwise continue to serve UK retail demand via a UK principal dealer. Such responses saw the proposed rule as a positive development which can help to foster the growth of a UK market ecosystem, and of UK-authorised execution venues.

3.37 Those who were unsupportive generally considered that more flexibility in order routing and execution venue selection is needed, as crypto liquidity is fragmented, global and often concentrated outside the UK. They acknowledged that the proposal is intended to ensure that consumers are serviced by appropriately regulated firms but were concerned that this approach would ultimately constrain consumers' ability to access deeper pools of liquidity and receive the best prices available on international platforms. We note that firms should separately consider the effect of the Cryptoassets Regulations, and that our rules cannot provide more flexibility where it is not aligned with Cryptoassets Regulations.

3.38 Over half of the unsupportive responses were critical of the proposed restriction on systematically or predominantly sourcing liquidity from affiliated overseas QCATPs. They considered that relying on the proposed conflicts of interest and best execution rules, coupled with supervisory oversight during the application process, would have been a more proportionate and targeted means to address the associated risks.

3.39 Some of those who were unsupportive also suggested that we should allow hedging on non-UK QCATPs if UK liquidity is insufficient, provided the principal dealer that executes an order is UK-authorised and retains full responsibility for best execution, governance, and client outcomes.

3.40 In addition, many respondents proposed that we should consider a proportionate equivalence or recognition framework. This is so that firms have more flexibility to access overseas, unauthorised liquidity sources that are subject to comparable regulatory standards in their local jurisdictions.

3.41 The feedback also stressed the general need for deferral measures, as respondents suggested that for a broad range of cryptoassets, there may be too few UK-authorised execution venues with sufficient liquidity at regime go-live.

Our response

Having considered the feedback carefully, we have proceeded with the proposed execution venue requirement, and the final rules and guidance provide additional clarity.

While we previously referred to the activity of receiving and transmitting orders for execution when consulting on this rule, in light of the feedback, we agree that this would leave a wide range of other arranging activities out of scope. For example, under the wording used in the CP, a UK-authorised arranger could continue to make arrangements with a view to retail clients transacting on overseas, unauthorised QCATPs which is not in line with our intended outcome (although the overseas firms in this case risk breaching the regulatory perimeter set out in the Cryptoassets Regulations). This gap poses significant risks of regulatory arbitrage and consumer harm. We have therefore amended the draft rule to close this gap in our final rules.

As a result, a firm must make sure that, when executing orders or receiving and transmitting orders for execution for a UK retail client or elective professional client, the order is executed on a UK-authorised execution venue.

For the same kinds of clients, where a firm is otherwise arranging deals in qualifying cryptoassets it must take all reasonable steps to ensure that the arrangements it provides only result in a client's order to be executed on a UK-authorised execution venue. In this case, the firm may, for example, consider the other firms to which clients are directed and whether such firms are required to comply with these rules.

In addition, when a firm executes orders for retail or elective professional clients as a principal, it must not systematically or predominantly source liquidity from a QCATP where the operator of that QCATP is in the same group as the firm and is not authorised as a UK QCATP operator. This requirement aims to disincentivise potential regulatory arbitrage by international firms.

These measures help keep consumer-facing services within the UK regulatory perimeter. They also make sure UK consumers are protected by conduct standards, market abuse controls, admission and disclosure requirements and supervisory oversight. They help reduce the risk of inadvertent perimeter breaches by unauthorised overseas firms too.

We acknowledge respondents' concerns around accessing global liquidity pools and efficient pricing. However, we consider that the proposed measures are essential in deterring regulatory arbitrage by unauthorised firms, which risks unfairly disadvantaging UK-authorised firms. A principal dealer managing its own liquidity positions is generally permitted to source liquidity from a wide range of global liquidity pools, ensuring pricing efficiency. Besides, these concerns have been addressed to some extent by our other proposed rules, such as allowing, under certain conditions, authorisation via a branch for overseas-incorporated QCATP operators where such a branch authorisation enables customer access to the firm's global liquidity pool.

As for the general ability of a UK authorised principal dealer to hedge its own positions on non-UK QCATPs if UK liquidity is insufficient (as raised by the feedback described in paragraph 3.39), we note that our proposals already permit this business model in most cases.

Related, we observed that some respondents struggled to fully interpret the concept of an 'execution venue'. In the final rules and guidance, we have clarified the meaning of this term, as this is a key concept underpinning these requirements. Where a firm executes client orders on a matched principal basis, the firm is not deemed to be a qualifying cryptoasset execution venue when only acting in that capacity to execute the orders. On the other hand, where a firm otherwise acts in a principal capacity when executing client orders, it should be considered as the qualifying cryptoasset execution venue.

This interpretation is aligned with established understanding in TradFi, where matched principal trading is treated as more akin to agency execution in scenarios similar to those that we are considering in crypto markets. As a result, a firm cannot set itself up to merely match orders on unauthorised QCATPs with UK retail client orders, ie as a "pass through". Otherwise, such arrangements may be artificially set up to help the unauthorised QCATPs avoid UK authorisation requirements and our rules while in effect serving UK retail clients.

Regarding a formal equivalence or recognition framework, we are not in a position to provide formal equivalence or recognition.

We have noted the requests for deferral arrangements and intend to consult on creating a deferral mechanism with respect to execution venue requirements, extending by 3 months, to January 2028, the time by which these rules must be complied with. We intend to consult on this in September of this year.

Question 12 – assets on which intermediaries can engage with UK retail clients

Consultation proposals

3.42 We proposed an admission to trading requirement. This limits the cryptoassets (other than UK-issued qualifying stablecoins), in relation to which cryptoasset intermediaries can serve UK retail clients, to those assets that are admitted to trading on at least 1 UK QCATP, and that have the relevant A&D-compliant Qualifying Cryptoasset Disclosure Documents (QCDDs) available.

3.43 In CP25/40 we asked:

Question 12: **Do you agree with our proposed restrictions on the cryptoassets in which an intermediary can deal or arrange deals for a UK retail client? If not, please explain why not?**

Feedback

3.44 We received 30 responses to this question. Feedback shows a roughly even split in sentiment (with 37% supportive versus 40% unsupportive) about our proposed restrictions.

3.45 Those who were supportive of our proposal saw it as an essential safeguard to ensure that retail clients benefit from an appropriate standard of disclosure and market oversight, as is the case in traditional financial markets. This mitigates the risk of regulated firms making questionable assets available to retail clients purely due to the popularity or market demand of such assets at a given point in time.

3.46 Other respondents, however, considered the proposal disproportionate. They argued it may limit the available routes to market for innovative token projects and create undue dependency on a potentially small number of UK QCATPs.

3.47 Several responses argued that whether an asset is listed on a UK QCATP may depend on factors such as commercial priorities, listing capacity and appetite, rather than the asset's underlying risk, governance or market integrity. So, they considered it likely that many assets may be liquid and credible, but not made available to UK retail clients via regulated channels as they are not admitted to trading on a UK QCATP.

3.48 Many respondents also emphasised the importance of appropriate deferral arrangements to help ensure sensible treatment of legacy holdings and mitigate potential cliff-edge effects.

Our response

We have considered the feedback carefully and have proceeded with the proposed restrictions largely as consulted on. This means before a firm can deal or arrange deals in qualifying cryptoassets (other than UK-issued qualifying stablecoins) for or with a UK retail client:

- The qualifying cryptoasset must be available to be traded by retail clients on a UK QCATP and must be admitted to trading on a retail UK QCATP in compliance with CRYPTO 3;
- The UK QCATP operator must have made available the QCDD and, where relevant, supplementary disclosure document for the qualifying cryptoasset in accordance with CRYPTO 3; and
- The qualifying cryptoasset must not have been withdrawn from trading on all UK QCATPs;

unless the firm is arranging deals in qualifying cryptoassets and arranges the sale of a qualifying cryptoasset offered on condition that the qualifying cryptoasset will be available to be traded by retail clients, and will be admitted to trading on a retail UK QCATP, and that the UK QCATP has made available the QCDD and, where relevant, supplementary disclosure document for the qualifying cryptoasset in accordance with Crypto 3.

We consider that these restrictions are essential for:

- The effectiveness of the broader A&D and MARC frameworks (PS26/9), which are foundational to the new cryptoasset regime.
- Consumer protection, by ensuring that retail clients who rely on regulated intermediaries access only assets that meet minimum standards of oversight and disclosure.

This approach also sets common standards across intermediaries, given that otherwise token-selection practices may naturally diverge based on each intermediary's risk appetite. Having in place these restrictions mitigates the risk of a 'race to the bottom'.

In addition, firms must make available to UK retail clients the QCDD and supplementary disclosure documents for the qualifying cryptoassets they deal or arrange deals in, before the client's initiation of the transaction. They also must make available to such clients the Stablecoins QCDD for any UK-issued qualifying stablecoin that they deal or arrange deals in, before the client's initiation of the transaction.

Where there are two or more relevant QCDDs, the firm should make all relevant QCDDs (and supplementary disclosure documents where applicable) available.

We have noted the requests for deferral arrangements and intend to consult on creating a deferral mechanism with respect to the admission to trading requirement, extending by 6 months, to April 2028, the period during which cryptoassets admitted on UK QCATPs (or on QCATPs in savings provision) can be sold to retail clients without a QCDD. We intend to consult on this in September of this year.

Rules to manage specific conflicts of interest

Consultation proposals

3.49 In CP25/40, we proposed that at least functional separation should be implemented between proprietary trading and client order execution. We set out that cryptoasset intermediaries who engage in payment for order flow (PFOF) would be unlikely to meet our requirements when they provide services to retail or professional clients. In addition, we proposed to apply personal account dealing rules to cryptoasset intermediaries.

Question 13 – Conflicts of interest during order execution

Consultation proposals

3.50 We expected that at a minimum, functional separation, including separate governance structures, should be required between firms' proprietary trading and client order execution operations.

3.51 In CP25/40 we asked:

Question 13: **Do you agree with our proposed approach to addressing conflicts of interest during order execution when a firm is engaged in proprietary trading? If not, please explain why not?**

Feedback

3.52 There were 28 responses to this question. Feedback on our proposed approach to addressing conflicts of interest during order execution was broadly positive, with 82% of responses supportive of the proposal. Respondents generally agreed that conflicts between proprietary trading and client order execution pose risks to clients' best interest, and functional separation can serve as a minimum mitigant.

3.53 Responses also emphasised that firms should be allowed flexibility to design specific conflict-management arrangements that fit their business models, provided they can demonstrate good consumer and client outcomes and evidence that controls are effective in practice.

Our response

Having considered the feedback carefully, we have proceeded with the proposal as consulted on. Firms are expected to design appropriate systems and controls to address any client detriment arising out of conflicts between the firm's qualifying cryptoasset proprietary trading and client order execution. Such measures are expected to include functional separation between these different types of trading.

Where conflicts cannot be mitigated or managed by functional separation alone, we expect firms to take additional measures to mitigate, manage and disclose such conflicts.

Question 14 – Payment for order flow (PFOF)

Consultation proposals

3.54 We expected that cryptoasset intermediaries engaging in PFOF are unlikely to meet our requirements such as best execution, conflicts of interest, and restriction on inducements, when they provide services to retail or professional clients.

3.55 In CP25/40 we asked:

Question 14: **Do you agree with our proposed approach to PFOF? If not, what carve outs do you consider necessary and why?**

Feedback

3.56 There were 25 responses to this question. 80% of responses were supportive of our proposed restrictions on PFOF. Respondents supported that, in most cases, PFOF is incompatible with best execution, conflict-of-interest rules, and fair competition, particularly when firms serve retail clients. They argued that firms receiving payments linked to order routing have an inherent incentive to prioritise their own revenue over execution quality for clients.

3.57 Many of these responses also argued that the case against PFOF is even stronger in crypto than in traditional markets. This is due to fragmented liquidity, opaque spreads and fees, and variable execution quality across venues. It is also challenging for clients, especially retail customers, to observe and assess execution outcomes. As a result, respondents were of the view that risks associated with PFOF cannot be fully mitigated by merely providing disclosures to clients.

3.58 20% of respondents were unsupportive of our proposed approach. They argued that PFOF remains a permitted and widely used market practice in the US, subject to disclosure requirements. They asked that the FCA avoid or defer any restrictions in the absence of conclusive empirical evidence.

Our response

Having carefully considered the feedback, we have included the proposals set out in the CP in our final rules and guidance. We expect that cryptoasset intermediaries engaging in PFOF behaviours are unlikely to meet our requirements such as best execution, conflicts of interest, and restriction on inducements, when they provide services to retail or professional clients.

We consider that PFOF presents risks to the effective management of conflicts of interest and inducements, in particular for some cryptoasset markets. It generates risks of consumer harm that individual firms may struggle to manage effectively.

We are also concerned that allowing PFOF may encourage crypto intermediaries to overly rely on a few liquidity providers that offer higher payments. This may harm market competition in the long run.

This approach aligns with our established approach towards PFOF for other regulated investments, and with the 'same risk, same regulatory outcome' principle.

Question 15 – Personal account dealing rules

Consultation proposals

3.59 We proposed to apply personal account dealing rules similar to those under COBS 11.7 to cryptoasset intermediaries.

3.60 In CP25/40 we asked:

Question 15: **Do you agree with the proposal to apply personal account dealing rules to cryptoasset intermediaries? If not, please explain why not?**

Feedback

3.61 All 27 respondents were supportive of our proposal to apply personal account dealing rules to cryptoasset intermediaries. Respondents saw such rules as an important mechanism to mitigate risks of insider dealing and unfair conduct, and to support market integrity and consumer confidence.

3.62 The feedback also contained broad support for our approach, which leverages existing personal account dealing rules. Respondents agreed that this approach would create a more familiar, enforceable and credible framework.

Our response

Personal account dealing by employees or individuals connected to a firm carries risks of conflict of interest between the individual and the firm or the firm's clients. Such conflicts can also extend to market abuse through misuse of confidential or inside information. So, we consider it necessary to introduce appropriate personal account dealing rules and have proceeded with this proposal as consulted on.

This means cryptoasset intermediaries must establish, implement and maintain adequate arrangements to manage conflicts of interest in relation to personal account dealing by any relevant person (for example a director, partner or manager of the firm). They must also make and keep records evidencing compliance with these requirements.

By way of reference, firms should also consider our requirements around the systems and controls of cryptoasset intermediaries to help prevent, detect, and disrupt market abuse in PS26/9.

Settlement

Consultation proposals

3.63 We proposed that intermediaries should have flexibility over whether they internalise settlement or arrange it externally, provided that they ensure clients understand the firm's settlement responsibilities. Where an intermediary is responsible for overseeing or arranging settlement, we proposed that it must have documented and published arrangements to mitigate settlement risk.

3.64 In CP25/40, we asked:

Question 16: **Do you agree with our proposed requirements on intermediaries around settlement arrangements, where applicable? If not, please explain why not?**

Feedback

3.65 We received 28 responses to this question. 86% of respondents were supportive of our proposed requirements around settlement arrangements. The other 14% of responses were either neutral or unclear.

3.66 Respondents supporting our proposal agreed that the proposed requirements can strengthen consumer protection by ensuring that firms take clear responsibility for, or provide clear disclosure on, how settlement is handled.

3.67 They also noted that the proposed approach gives firms flexibility over whether they internalise settlement or arrange it externally. They preferred this approach as it recognises the diversity of business models and technological infrastructures in cryptoasset markets.

3.68 The neutral or unclear responses mostly commented on the wider settlement or safeguarding rules that go beyond this consultation question. These have been addressed in other relevant chapters of this Policy Statement instead.

Our response

We have proceeded with the proposed requirements as consulted on. This means where applicable, for example when an intermediary firm takes responsibility for arranging the settlement of an executed order, it must clearly inform the client of the process for the settlement of the respective transaction, including any associated risks. Where a firm provides the service of arranging or otherwise bringing about settlement of a qualifying cryptoasset transaction, we expect the firm to initiate the final settlement of the transaction within 24 hours of the transaction being executed.

Firms should also consider the broader safeguarding rules in Chapter 7: Safeguarding of this PS. Further, the cryptoasset perimeter guidance consultation in CP26/13 sets out our proposed expectations for firms seeking to rely on the temporary settlement exclusion from the perimeter of the safeguarding activity. This exclusion is provided for in Article 9Q of the Cryptoassets Regulations.

Chapter 4

Pre- and post-trade transparency

4.1 This chapter summarises the feedback on our proposed transparency requirements for cryptoasset trading platforms and intermediaries set out in Chapter 4 of CP25/40 and describes our response.

Overview of CP25/40 consultation proposals

4.2 As we explained in CP25/40, trade transparency to the market can support better execution outcomes and market integrity by improving price discovery.

4.3 So, we proposed that UK QCATPs, as well as principal dealing firms, are required to provide pre-trade transparency to the market if the firm exceeds a certain size threshold. We proposed that UK QCATP operators publish the best 5 bids and offers, along with corresponding volumes, for each cryptoasset pair. For firms dealing as principal, we proposed publication of firm quotes to clients. We proposed the required information be published as it arises either for free or on a reasonable commercial basis. Firms opting for the latter should publish information for free in a machine-readable format 15 minutes following initial publication.

4.4 The size threshold above which we proposed pre-trade transparency would be required was ≥£10m per annum average annual revenue at entity level, measured over a 3-year rolling period. This was intended to make sure that transparency is provided by the larger firms, which collectively account for most of the market's transaction volume, without imposing potentially disproportionate financial and operational complexity burdens on smaller firms.

4.5 We also proposed that all UK QCATPs and principal dealing firms should provide post-trade transparency to the market, including at a minimum: date and time of transaction, venue and cryptoasset ID, instrument price and reference currency or reference cryptoasset for that price, quantity of cryptoassets, and date and time of publication of the transaction.

4.6 This information should be published as close to real time as is technically possible, and in any case within 1 minute of execution. As for pre-trade, the information could be published for free or on a reasonable commercial basis, and where published on a commercial basis, would have to be offered for free 15 minutes after initial publication.

4.7 We further proposed to limit applicable transparency requirements to transactions that are most relevant for price formation and where real-time disclosure is not likely to harm client interests by:

- Carving out certain business models and activities (eg issuance and redemption of liquid staking and wrapped tokens) from pre-trade transparency requirements.

- Allowing firms to establish their own policies for pre-trade transparency waivers and post-trade transparency deferrals to use where transactions would likely have a significant market impact.

4.8 In CP25/40 we asked:

Question 17: **Do you agree with our proposed pre-and post-trade transparency requirements for UK CATP operators and principal dealers? If not, please explain why not?**

Question 18: **Do you agree with our proposed methodology for determining the pre-trade transparency threshold? If not, please explain why not? What other methodology do you suggest?**

Question 17 – pre- and post-trade transparency requirements

Feedback

4.9 There were 45 respondents to this question. 62% of respondents were generally supportive of pre- and post-trade transparency requirements. They agreed that it offers benefits such as more efficient price discovery, competition, and market integrity.

4.10 Of the 20% of respondents that were unsupportive, most raised concerns in relation to the obligations on principal dealers:

- On pre-trade, 5 (11%) respondents objected to the inclusion of principal dealers in the scope of pre-trade transparency requirements. They argued that including principal dealers in scope of pre-trade transparency rules would be misaligned with recent TradFi reforms to the Systematic Internaliser (SI) regime for bonds and derivatives which removed the requirement.
- On post-trade, 3 (7%) respondents raised concerns that the requirement to publish post-trade information within one minute was disproportionate to the maturity of crypto markets. They suggested that a 15-minute window for post-trade reporting would be more appropriate. They argued that this would align with the timeframe required at the start of post-trade reporting on bonds and derivatives under the SI regime.

4.11 5 (11%) respondents were unsupportive of our proposals to enable firms to create their own policies for waiver/deferral application. They stated this could lead to a lack of standardisation and called for more prescriptive rules and further guidance, including on restrictions for the use of deferrals, to ensure consistency.

4.12 One respondent argued that deferrals should also be allowed where timely post- trade transparency would adversely affect a dealer's own trading interests, rather than being available only where the effect is on the trading interests of clients.

Our response

We have not proceeded with our proposal to require pre-trade transparency to the market from principal dealers. Our decision follows consideration of feedback from respondents and aligns with the recent changes to the SI regime for bonds and derivatives in TradFi (see PS24/14 and PS25/17). We do not expect this to have a material impact on the efficiency of price formation at this stage, as most of the current UK crypto volume is transacted on QCATPs. However, we intend to monitor how the market structure and dynamics evolve from here and may review this policy in due course. We note that in TradFi, pre-trade transparency requirements remain in place for equities principal dealers.

However, we have proceeded with pre-trade transparency obligations for large UK QCATP operators. QCATPs currently are the primary liquidity centres for UK clients and so play an important role in efficient price formation and market integrity, ultimately supporting better consumer outcomes.

We have also proceeded with our post-trade transparency proposals. This means all QCATP operators and principal dealers must publish post-trade information as close to real time as is technically possible and at most within 1 minute of execution. These requirements reflect consideration of EU crypto regulations where trading platform operators must publish post-trade data within 30 seconds, and TradFi rules where equities post-trade information must be published within 1 minute of execution.

We have also proceeded with our proposals for waivers and deferrals but have not provided more detailed requirements or guidance at this stage. We are conscious of the need to accommodate the diverse and rapidly developing number of business models within the industry. This approach allows firms to create their own policies, which comply with our rules, while simultaneously permitting the flexibility required for a range of business models.

We have clarified post-trade transparency deferrals to include where a dealer, with respect to its ability to offer prices to clients, may need time to hedge large or illiquid positions.

Question 18 – size threshold for pre-trade transparency

Feedback

4.13 There were 40 respondents to this question. 39% of respondents did not support the proposed pre-trade transparency threshold. These respondents generally argued that:

- Basing the threshold on total entity revenue from all business activities is too broad; instead the calculation should be based on revenue from cryptoasset-related activities so that firms for whom crypto activity constitutes the minority of their overall business do not fall within scope.
- Revenue is not an adequate indicator of a firm's role in price formation; instead respondents proposed various more nuanced and complex alternatives, such as basing the threshold on factors including trading volume and trade size.

4.14 17 (43%) respondents supported the proposal and noted the benefits of a less complex threshold, as well as the need to ensure requirements are proportionate for smaller firms.

4.15 3 (8%) respondents argued that all firms should be subject to pre-trade transparency, with some suggestions that a lack of transparency for smaller firms may attract liquidity from those wanting to avoid the increased transparency.

Our response

We have proceeded with the ≥£10 million revenue threshold for pre-trade transparency. However, this only applies to QCATP operators since principal dealers will be out of scope of pre-trade transparency (see Our response to question 17, above).

We have maintained the methodology for calculating the threshold as proposed in the CP, including a 3-year rolling average to calculate revenue, which supports predictability of firms' market entry and growth decisions. We believe the benefits of simplicity outweigh the costs in this instance.

In response to the suggestion that a lack of transparency for smaller firms could lead to a concentration of liquidity on such venues from those wanting to avoid transparency, we note that:

- If this were to happen, such venues would eventually exceed the revenue threshold.
- We will monitor the evolution of market structure and will review the rules should this become necessary, as noted in Our response to question 17, above.

Chapter 5

Record keeping and client reporting

5.1 This chapter summarises our proposals, feedback, and our response, for record keeping and client reporting obligations on UK QCATPs and intermediaries.

5.2 Unlike in similar situations in TradFi, and as we explained in CP25/40 and CP25/41, the FCA will not systematically receive or assess individual cryptoasset order or transaction data.

Overview of CP25/40 consultation proposals

Transaction/order record keeping

5.3 We consulted on requiring firms to record a minimum set of information on each order and transaction. We proposed that this information be retained for 5 years, in line with the requirements under MARC and more broadly record-keeping obligations attaching to trading venues and firms under UK MiFIR. The minimum set included data to identify the nature of the order or transaction, all parties involved, the cryptoassets involved, and information on price, volume and timing of execution. The draft instrument included a full list of the minimum required datapoints.

5.4 We said that firms should assess whether the minimum requirements would be sufficient for the firm to meet its regulatory obligations under MARC, the MLRs, and the incoming Cryptoasset Reporting Framework (CARF), and that they should retain additional information should this be necessary.

5.5 By way of context, the CARF requires UK reporting cryptoasset service providers (RCASPs) to collect information in relation to in scope transactions on an annual basis. CARF is based on Organisation for Economic Co-operation and Development's (OECD's) 2023 publication entitled 'International Standards for Automatic Exchange of Information in Tax Matters: Crypto-Asset Reporting Framework and 2023 update to the Common Reporting Standard'. This was implemented in the UK through secondary legislation and came into effect on 1 January 2026.

5.6 We noted that firms must be able to provide relevant records required under our proposals to the FCA upon request. To support comparability of data, we also specified certain requirements for how data should be formatted (eg requiring that execution date and time be expressed in UTC and detailing how to create a personal identifier for the purposes of these records where no recognised identifier, such as a national insurance number, is available or used). However, we did not provide detailed data standards/ formats in which the information is to be recorded and retained on the basis that firms are best placed to determine what is needed for their business.

Client reporting

5.7 We proposed that UK QCATP operators and intermediaries should report to their immediate clients on the execution of their orders promptly and, at the latest, at the end of the day when the order was executed or the information received.

5.8 We specified client reporting should be provided in a durable medium, storable for future reference and we listed the minimum essential information that should be reported to clients. This included both firm and client identifiers, the identifier of the cryptoasset(s) to which the order or transaction relates, the quantity and nature of the order/transaction (eg buy or sell), details on execution date and time; and price, costs and charges, as well as total consideration.

5.9 We also consulted on requirements that firms:

- Should report details of specific instructions given by the client (since such instructions could mean the firm has executed the order in question in a different way than would normally be expected under best execution).
- Should include orders that have been cancelled and provide the reason for the cancellation in their client reporting.
- Would be allowed not to report where clients had opted out of receiving reports entirely or (subject to certain conditions) only report those essential elements of information that are not easily available on chain.
- Should give clients access to a 3-year history of their transactions on request.

5.10 In CP25/40 we asked:

Question 19: **Do you agree with our proposals for transaction recording and client reporting requirements for UK CATP operators and intermediaries? If not, please explain why not?**

Feedback

5.11 There were 38 respondents to this question. 85% of respondents supported our proposals and the remaining 15% were neutral. Despite this overall support, respondents provided certain targeted suggestions on the 2 topics covered by the question.

Record keeping and client reporting

5.12 Most of the suggestions related to ensuring alignment with other record keeping/reporting standards, including under MARC, the MLRs, HMRC's CARF) and international regimes.

5.13 Related, several respondents also suggested that we provide more guidance on data standards, reporting formats and interoperability expectations.

5.14 Further, some firms suggested that record keeping and/or client reporting requirements should be lighter touch for either or both, arrangers to non-custodial wallets and occasional (as opposed to systematic) dealers.

Record keeping only

5.15 Several respondents offered suggestions on specific data to be recorded:

- Some proposed to add a requirement to record data (such as transaction hashes and wallet addresses) that would ensure that the link between on- and off-chain records can be re-established when needed.
- One respondent said that the proposed requirement to record decision makers was too onerous, but two others thought that it was appropriate.

5.16 Some respondents raised concerns over the possibility of data breaches that could affect the security of personal data, given the recording of personal identifiers. They suggested that pseudonymisation should be allowed (provided pseudonyms can be linked back to the underlying person if needed).

5.17 One respondent urged the FCA to consider requiring transaction reporting to the regulator.

Client reporting only

5.18 Several respondents raised concerns about intermediaries' ability to comply with the client reporting proposals strictly as set out in CP25/40. Concerns included:

- Agents and arrangers may not have the data to fulfil all the client reporting requirements.
- Intermediaries may also struggle to meet the T+0 timing requirement for client reporting. Respondents argued that this could be difficult because intermediaries may be dependent on the execution venue (ie a QCATP or a principal dealer) to provide them with certain details (eg execution timing), and where these details are received late, the intermediary's onward reporting to the client would then also be late.

5.19 Respondents also requested further guidance and/or clarification of certain requirements, including:

- Confirmation that 3-year lookback access to be given to clients for their own transaction history can be subject to ID verification and rate limitation.
- Confirmation that a 'durable medium' for reporting information to clients can include interfaces allowing clients to export their data to standard file formats.
- Further guidance on the meaning of information being 'readily available on chain' where a firm relies on this as the reason for not reporting the information to the client separately.

5.20 Some respondents commented on the proposed content of client reporting:

- One firm felt it was overly onerous to include the details of any specific instructions given by the client in relation to a particular order.
- Another suggested that we include additional data such as the capacity in which a venue executed a particular trade (eg by internalising the risk as a principal dealer or passing it on); any conflicts that may have applied; and details on the settlement method.

Our response

Record keeping and client reporting

We have considered the suggestions for more alignment and standardisation. As a result, our final rules require that individual cryptoassets are identified by their Digital Token Identifier (DTI) (ISO 24165) in the first instance, in both order/transaction records and in client reporting. This is in line with A&D requirement that QCDD documents include a DTI. The exception to this requirement may be an asset that can only be sold to institutional clients and therefore would not be required to be admitted to trading with an A&D compliant QCDD nor to have a DTI. For such an asset, if it does not have a DTI, we have retained our original proposal that the reporting can include an alternative unique and unambiguous identification code for each qualifying cryptoasset involved in an order/transaction.

We have not provided further guidance on data standards, reporting formats, and interoperability expectations at this stage, because we believe given the rapid pace of change, the global nature and the still early stage of development of the industry, it would be premature for the FCA to impose a particular standard. However, we would welcome industry initiatives to drive standardisation forward in due course.

We also have not varied record keeping and client reporting requirements for smaller firms, occasional traders or certain business models, because:

- The information we require firms to record is important to support effective detection and investigation of market abuse and ensure clear accountability. Without the ability to detect and investigate market abuse across all participants, there would be a risk that bad actors could migrate to, eg smaller firms with an intention to avoid detection and this could lead to poor outcomes for clients of such firms and could undermine overall market integrity.
- Similarly, reporting a full set of information to clients is critical for allowing clients to evaluate the service provided to them. Reducing reporting where firms serve clients less often would inappropriately disadvantage these firms' clients.

In addition, we draw firms' attention to Our response to question 11 (Chapter 3, above). This confirms that, in line with TradFi, where an intermediary executes client orders on a matched principal basis, the firm is not deemed to be a qualifying cryptoasset execution venue when only acting in that capacity to execute the orders. So, the matched principal dealer's record keeping and its client reporting (where applicable) would need to identify the ultimate venue as the execution venue.

Record keeping only

We have considered the suggested changes to the minimum set of data that we require firms to record and retain. We have updated our final rules to incorporate the suggestion to require the recording of transaction hashes and associated transaction addresses, such as wallet addresses and smart contract addresses, where applicable, and network fees. In addition, we remind firms that:

- Our specific requirements are intended to serve as a baseline of what must be recorded.
- They must have systems and procedures in place to assess whether they need to record and retain any additional information in relation to client orders and transactions to comply with their obligations.

We have retained the requirement to record the decision maker for a given order in the firm placing the order. This information is important to ensure clear accountability and support effective detection and investigation of and enforcement against market abuse. We therefore consider this requirement to be proportionate in light of the risk it is helping to address.

We have also retained our existing proposals in relation to recording and retaining personal identifiers. However, where firms have concerns that sharing such information could conflict with applicable data protection requirements, we draw attention to the guidance at CRYPTO 4.9.14 in the MARC rules, which clarifies that our requirements should be interpreted consistently with firms' obligations under wider legal obligations.

We have not changed our approach to transaction reporting to the FCA because at the current scale of cryptoasset markets, we consider that the appropriate role for us is to oversee the compliance of QCATP operators and intermediaries with market abuse rules. However, this does not preclude the possibility of authorised QCATP operators and intermediaries reporting suspected cryptoasset market abuse to us only if they have reasonably concluded that the suspected market abuse activity could not be adequately prevented, detected or disrupted by appropriate measures available to them. We also have the ability to take appropriate action against firms who do not comply with our rules. We would expect authorised firms to comply with Principle 11 in our Handbook and disclose to us appropriately anything relating to the firm of which we would reasonably expect notice.

We also note that while we have not required transaction reporting to the FCA, firms are subject to general regulatory reporting requirements (discussed in PS26/13). Other relevant financial crime reporting obligations, such as those under the MLRs or the Proceeds of Crime Act 2002, for example, also continue to apply.

Client reporting only

Responding to the concerns raised about intermediaries' ability to provide clients with the required reporting, we note that:

- The 'same day' reporting requirement already provides that firms receiving information from another firm to enable their own client reporting (as would be the case for certain intermediaries) must report on the day that they themselves receive the information. This protects these firms in case the data is provided to them with a delay. In addition, we have refined our rule to account for the possibility of data being received very late in the day by limiting the 'same date' reporting requirement to transactions that are executed, orders that are cancelled or data that is received before the end of the working day. Where execution, cancellation or data receipt happens after the end of the working day, reporting can be delayed to the following working day.
- Where certain intermediaries (such as agents and arrangers) may not themselves have all the data needed immediately available to meet their client reporting obligations, they should put in place arrangements to obtain the required data from the ultimate execution venue.

As to the requests for further guidance and/or clarification, we:

- Confirm that the purpose of the provisions in CRYPTO 8 is to enable consumers to request personal sensitive information to consider and assist with their investment decisions/administration. As such it is reasonable and necessary that acquiring such information is appropriately protected, eg by authentication. Albeit, such protections should not impede a consumer's access 'at any time' to their information upon request, as contemplated and required by CRYPTO 8.3.5R.
- Have expanded on our rule to clarify that the information required under CRYPTO 8.3.5R to be delivered in a durable medium can be delivered by means of a website, mobile application or any other digital medium in accordance with the website conditions, to the extent it is not a durable medium.

As for the suggested changes to data required to be reported to clients, we have:

- Retained the obligation to reference specific instructions, where applicable, as this enables clients to identify if best execution was disapplied inappropriately.

- Added a requirement to indicate the settlement method in client reporting.
- Not required reporting on conflicts or the capacity in which a venue executed a particular trade (except for the scenario set out earlier in Our response to question 19 above) as conflicts and the general capacity in which a firm engages with a client already need to be disclosed at other points in the customer journey.

Chapter 6

Lending and borrowing

6.1 This chapter sets out the requirements for firms engaged in cryptoasset lending and cryptoasset borrowing ('L&B') activities.

6.2 Cryptoasset lending and cryptoasset borrowing are industry terms for certain cryptoasset services. Firms offering these services may be engaged in various regulated activities, such as, 'dealing in qualifying cryptoassets as principal', 'dealing in qualifying cryptoassets as agent' and/or 'arranging deals in qualifying cryptoassets'. We have used industry terms to make sure that firms who offer these services are aware that FCA requirements apply to these activities when they involve retail clients and that they must comply with the relevant rules. In all circumstances, firms should look to the nature of the activities they perform to consider whether they need to be authorised to conduct those activities.

6.3 When we use the term cryptoasset lending, we mean the disposal of a qualifying cryptoasset from a person to or via an authorised cryptoasset firm subject to an obligation or right to reacquire the same or equivalent qualifying cryptoassets from the firm, typically with compensation paid to that person by the firm in the form of yield.

6.4 When we use the term cryptoasset borrowing, we mean the disposal of a qualifying cryptoasset from or via an authorised cryptoasset firm to a person subject to an obligation or right to reacquire the same or equivalent qualifying cryptoasset from the person, which may include the provision of qualifying cryptoasset borrowing collateral and/or payment of interest from the person to the firm.

6.5 To be clear, L&B services are not lending or borrowing services in the traditional sense. In L&B, the provision of the service involves a disposal of the assets to the recipient, where the assets then become the property of the recipient. In cryptoasset lending, the firm is the recipient and, in cryptoasset borrowing, the client is the recipient. This is often not the case in traditional lending and borrowing.

6.6 We appreciate these terms may not be intuitive, particularly for those who are more familiar with the definitions of lending and borrowing used in traditional finance. We believe the consumer understanding rules we are putting in place will make sure firms are clear in how they communicate, so that retail clients understand the nature of the service, no matter what terminology is used.

Proposals for cryptoasset L&B

6.7 In CP25/40 and CP26/4 we proposed requirements which would apply to L&B activities when these activities involve retail clients, with a view to balancing consumer protection and the provision of information to allow clients to determine the level of risk relevant to their individual circumstances. To summarise, we proposed:

- Information requirements that make sure retail clients receive clear, timely and comprehensible information about L&B services, including risks and costs.
- Key terms of agreement and express prior consent requirements that require firms to obtain express prior consent from retail clients to the key terms of L&B services each time a L&B service is provided.
- Appropriateness testing to make sure firms assess whether a retail client's knowledge and experience make them an appropriate customer before providing L&B services.
- Additional record-keeping requirements for L&B firms to supplement existing COBS and CASS record-keeping obligations (where applicable).
- Prohibiting the use of proprietary tokens in relation to L&B services provided to retail clients, due to conflict of interest, valuation, and market integrity risks.

Consumer understanding

6.8 In CP25/40 and CP26/4, we consulted on rules that we considered would improve consumer understanding of L&B services. We proposed these would be implemented through both COBS and the new CRYPTO 9 rules.

6.9 In CP26/4, we consulted on guidance saying firms have flexibility in how their systems and operations discharge the requirements set out in the draft CRYPTO 9 rules and COBS, noting that some of these obligations may overlap because they are both aimed at achieving similar outcomes.

6.10 In CP26/4, we asked:

Question 17: **Do you agree with our proposals on express consent, appropriateness testing, and strengthening retail clients' understanding? If not, please explain why not. If there is an issue of timing or cost in relation to our proposals on appropriateness assessments and express consent, including as they apply to existing clients, please share details.**

6.11 We also proposed requirements in CP25/40 that mean retail clients would receive information regarding their L&B service, so they can understand applicable risks.

6.12 In CP25/40, we asked:

Question 20: **Do you agree with our proposals on strengthening retail clients' understanding and express prior consent? If not, please explain why not.**

Feedback

6.13 We received 24 responses to Q17 in CP26/4. 83% supported our proposals and 17% did not support. Some respondents raised concerns over proportionality, arguing that retail clients engaging with L&B services are likely to be more experienced, so the additional appropriateness tests were unnecessary.

6.14 We received 33 responses to Q20 in CP25/40. Most respondents (82%) supported our proposals.

6.15 A large number said that information provided to retail clients should use easily comprehensible terms and plain English. Respondents expressed concern that repeated information and consent requirements could lead to clients experiencing 'click-through fatigue', reducing the effectiveness of the proposed requirements.

6.16 A small number of respondents (12%) did not support our proposals. They cited our proposal to require express prior consent before each transaction, with some preferring a one-time consent model where clients only provide consent at the commencement of their relationship with the firm.

Our response

Appropriateness Testing

We are proceeding with our proposal to require appropriateness testing for L&B services. We acknowledge the proportionality-related feedback we received in CP26/4 on the application of appropriateness tests for L&B services. However, having considered the feedback, our position remains that L&B services have specific risks compared to other cryptoasset services. So, it is important to assess whether a retail client's knowledge and experience make them an appropriate user of these services, to avoid negative outcomes for clients who do not meet the appropriateness threshold.

We recognise respondents' feedback that L&B users are typically more experienced, however, the function of the appropriateness test is to provide additional protection for retail clients who are not sufficiently knowledgeable or experienced to take on the type of financial risk these services can entail. Firms should not be offering L&B services to retail clients until the firm has assessed that it is appropriate to do so. The appropriateness tests are not designed to restrict more experienced retail clients from accessing L&B services.

Information disclosure

We are proceeding with the proposals requiring firms to provide retail clients with information before the client is bound by any agreement or before the provision of any L&B services, as consulted on. These requirements will help make sure firms provide retail clients with sufficient information to understand the L&B service they are accessing and to make informed decisions.

We have provided guidance setting out that firms may use a single set of systems to discharge the requirements set out in CRYPTO 9 and COBS. This guidance is set out in CRYPTO 9 and repeated in CRYPTO 10.

Express prior consent

We are proceeding with our proposals to require that firms obtain express prior consent from retail clients before the client is bound by any agreement or before the provision of any L&B services, as consulted on. We have considered the feedback on a one-time consent model. However, due to the risk profile and complexity of L&B services, we do not believe that this would be proportionate to the risk posed to retail clients.

We have considered respondents' feedback on the risk of repeated consent requirements leading to 'click-through fatigue'. As set out in COBS 4.5A.3, firms should make sure the information provided to retail clients uses simple, easily understood language so that it is clear which activity they are engaging in, and what the risks associated with this activity are. Firms must also have regard to the Consumer Duty and make sure that clients receive the information they need, at the right time, and in a way they can understand.

Use of proprietary tokens for L&B

6.17 In CP25/40, we outlined our proposals on the restriction of the use of proprietary tokens for L&B services provided to retail clients, citing conflict of interest and price manipulation risks. We asked:

Question 21: **Do you agree with our proposal to prohibit the use of proprietary tokens for L&B as outlined above? If not, please explain why not.**

Feedback

6.18 Overall, we received 29 responses to this question. These were mixed, with 41% of respondents supporting and 41% not supporting. Respondents who were supportive generally accepted our judgement that the use of proprietary tokens in L&B creates the potential for conflicts of interest and cannot be suitably managed by a firm, which would increase the risk to clients.

6.19 Respondents who were unsupportive felt that a full prohibition would be disproportionate and that the risks posed to retail clients could be mitigated by additional requirements and safeguards, and enhanced firm disclosures. Some respondents also noted that the scope of this rule should not include tokens with utility, such as governance tokens, utility tokens, user interface tokens, and other types of tokens which do not have any monetary or exchange value.

Our response

We appreciate the feedback and the use cases provided by respondents. After careful consideration, we have decided that the mitigations proposed by respondents, such as additional requirements and enhanced firm disclosures, would not adequately address the risks of consumer harm. Accordingly, we are proceeding with prohibiting the use of proprietary tokens in relation to L&B services provided to retail clients, as consulted on.

CRYPTO 9 defines a proprietary token as a qualifying cryptoasset that is not a UK-issued qualifying stablecoin and is issued by the firm or a member of its group, or is a qualifying cryptoasset over which the firm or a member of its group has a material control of its supply. The tokens that are within this definition are in scope of the prohibition. We are not applying it to other types of tokens, such as those outlined in paragraph 6.19.

Firms should note that the restriction on the use of proprietary tokens does not apply to L&B services provided to non-retail clients.

Record-keeping requirements

6.20 In CP25/40, we proposed additional record-keeping requirements for firms offering L&B services to any client, which include, where relevant, the amount of qualifying cryptoasset provided or received for each client, the amount of yield earned, the total fees charged, and the total amount of cryptoassets lost due to operational disruptions. These requirements are intended to supplement the record-keeping requirements in other areas of the Handbook, such as COBS 8 and CASS, and to make sure that there is alignment in the data being recorded across all L&B services.

6.21 In CP25/40, we asked:

Question 22: **Do you agree with our proposed record-keeping requirements on regulated L&B firms? If not, please explain why not.**

Feedback

6.22 Overall, we received 32 responses to this question. Most respondents (75%) supported our proposal. The 9% of respondents who were unsupportive cited concerns over client privacy and compliance challenges for firms. Some respondents saw these requirements as onerous and suggested the FCA should rely on on-chain records instead.

Our response

After consideration of feedback, we have decided to proceed with our proposals to require L&B firms to comply with the additional record-keeping requirements set out in CP25/40. We consider these requirements are essential for firms to maintain operational integrity, to enable effective oversight of firms, and to help prevent poor outcomes for clients.

We believe that issues surrounding client privacy should be sufficiently managed by data protection requirements, which firms are subject to. It is also our position that records on a public blockchain will not be sufficient for maintaining records of poor client outcomes, such as errors in calculating yield, fees, charges or commissions.

Proposals for cryptoasset borrowing

6.23 Alongside the proposals for L&B, we also proposed some cryptoasset borrowing-specific proposals in CP25/40 and CP26/4 for services provided to retail clients. These additional proposals were designed to address the unique risks of cryptoasset borrowing and the treatment of collateral. To summarise our proposed rules for cryptoasset borrowing, we proposed:

- Express prior consent must be obtained before a retail client's collateral is supplemented or topped up.
- Limiting the amount of additional collateral that a cryptoasset borrowing firm can supplement their clients' position to 50% of the market value of the initial collateral provided at the beginning of the cryptoasset borrowing service.
- Mandatory over-collateralisation to make sure the value of the collateral provided exceeds the value of the qualifying cryptoassets the retail client borrows from the firm.
- Managing the limits and levels of the loan by modelling the LTV ratio of the loan, the margin call level, and the liquidation level, such that a margin call or liquidation is not expected within the first 6 months of the cryptoasset borrowing service.
- Negative balance protection to make sure that the retail client cannot lose more than the collateral they have specifically dedicated for the purposes of engaging in cryptoasset borrowing.

- Collateral is safeguarded at all times by a firm with the appropriate permission to do so and in accordance with the relevant CASS rules that apply to the type of assets or money provided as collateral. We proposed this to prevent the firm from taking full title of the collateral and reusing it for their own account, ensuring full title remains with the retail client and that the collateral posted would be available when the terms of the cryptoasset borrowing arrangement have been fulfilled.

6.24 In CP25/40, we asked:

Question 23: **Do you agree with our proposals on additional collateral, mandatory over-collateralisation of retail clients' loans, and managing the limits/levels of the loan? If not, please explain why not.**

Question 24: **Do you agree with our proposals on negative balance protection? If not, please explain why not.**

Feedback

Collateral and loan limits & levels

6.25 Overall, we received 33 responses to the question on mandatory over-collateralisation of retail client loans and managing loan limit levels. Our proposal was supported by 76% of respondents, with 12% not supporting. Many respondents requested further guidance and clarification on modelling and managing the limits and levels of loans. Of those respondents that did not support our proposals, some raised the point that mandatory over-collateralisation would restrict the ability for firms to offer margin trading services to retail clients.

6.26 On managing the loan limit levels, several respondents mentioned the 50% restriction on the amount firms can supplement the collateral on the retail client's behalf. Whilst some respondents reacted positively, describing the proposal as practical and sensible, others felt it could lead to early liquidations, crystallised losses and reduced consumer choice.

Negative balance protection

6.27 Overall, we received 31 responses to the question on negative balance protection. 74% of respondents supported our proposed rules and 6% did not support them. Respondents that were unsupportive felt that firms should have access to retail clients' cryptoassets beyond the collateral that is specifically allocated for borrowing, citing the risk that this requirement could lead to earlier or more frequent liquidations.

Our response

Collateral and loan limits & levels

We are proceeding with our proposed rules on mandatory over-collateralisation of retail client loans and managing loan limit levels. These requirements will help make sure clients have sufficient assets to support the loaned value and reduce the risk of margin calls or liquidation in the first 6 months of the loan. We have considered the requests for additional guidance on this rule, but at this time we are not enhancing our guidance. Noting our commitment to make sure our rules are principles-based and outcomes focused, we believe it is important to allow firms to be flexible and innovative. Providing detailed, prescriptive guidance goes against our commitment in this area.

We note that some respondents raised the impact of mandatory over-collateralisation on the ability of firms to offer margin trading or leveraged services. For clarity, we can confirm that it is our intention to limit the provision of these services to retail clients by firms, as we believe that the risk profile and complexity of these services make them unsuitable for most retail clients. We do, however, recognise that the risks and market dynamics in this fast-moving sector continue to evolve. So, we will keep this under review as part of our evaluation of the regulatory regime.

We are proceeding with our proposed rules requiring firms to seek express prior consent before the firm can supplement the collateral on the retail client's behalf, and on limiting the amount the firm can supplement the collateral in this way to 50% of the market value of the original collateral provided by the retail client. These requirements will mitigate the risk of client losses in the event their collateral declines in value due to price fluctuations.

While we are proceeding with our proposal to limit the amount the firm can supplement the collateral on the retail client's behalf to 50% of the value of the initial collateral, we do not intend to prevent retail clients from supplementing their collateral themselves above this 50% threshold. We believe this promotes consumer choice by enabling clients to top up their collateral to avoid liquidation. Firms should be aware of requirements such as the Consumer Duty, where firms are required to act in good faith towards retail clients (PRIN 2A.2.1R) and avoid causing foreseeable harm (PRIN 2A.2.8R).

Negative Balance Protection

We are proceeding with our proposals on negative balance protection. This proposal prevents retail clients from losing more than the amount they have specifically dedicated for the purposes of engaging in cryptoasset borrowing. This proposal, alongside other rules, will encourage firms to model loan limits appropriately. This proposal is aligned with our negative balance protection rule for CfD trading under COBS 22.5.17R.

Applying CASS to L&B

6.28 We considered how the safeguarding rules in CASS 17 would interact with cryptoasset L&B services in CP26/4. For the assets transferred to firms by clients during a cryptoasset lending service, we proposed that CASS 17 should not apply. For the assets posted as collateral during a cryptoasset borrowing service, we proposed that firms must not take ownership of the collateral provided by a retail client, except where the client has consented for this to discharge their debt to the firm. Depending on the form of the collateral (ie qualifying cryptoasset, specified investment cryptoasset, security or contractually based investment, or money), the firm offering the borrowing service should make sure they have the appropriate permissions to either safeguard the collateral themselves or arrange for the collateral to be safeguarded.

6.29 In CP26/4, we asked:

Question 27: **Do you agree with our proposed approach to applying CASS 17 in these scenarios [L&B]? If not, why not, and please describe any scenarios we may not have considered.**

Feedback

6.30 Of the total respondents who addressed the application of CASS 17 to other activities, only 9 specifically addressed L&B. Of these, 44% were supportive, 33% were neutral or unclear, and 22% were not supportive.

6.31 For cryptoasset lending specifically, there was broad agreement that CASS 17 should not apply to the assets that clients transfer to firms, with 1 respondent raising concerns over consumer protections and disclosures.

6.32 For cryptoasset borrowing, 2 respondents felt that restricting title transfer of the collateral posted in cryptoasset borrowing was unnecessary. They argued that, provided the firm obtains the express prior consent from the retail client, the firm should be allowed to take full title transfer or treat the asset as its own until the end of the borrowing arrangement, even if it may only be for low-risk revenue generation activities. These respondents stated that this would be positive for the market, as it would provide liquidity and decrease borrowing costs for retail clients.

Our response

After considering the feedback carefully, we are continuing with our proposals that CASS 17 will not apply to qualifying cryptoassets that are transferred to the firm under a cryptoasset lending arrangement.

For qualifying cryptoasset borrowing, and the collateral posted as part of the arrangement, we are clarifying our proposals. For cryptoasset borrowing collateral posted by a retail client, the final rules set out that the collateral must be safeguarded or arranged to be safeguarded by the firm providing the borrowing service. This will mean that the collateral

is held on trust for the benefit of the client at all times. Ownership of the collateral cannot be transferred to the firm or any other party. The exception to this is where the firm can take ownership of the asset to discharge the indebtedness of the retail client.

Our proposals for the treatment of retail client cryptoasset borrowing collateral do not restrict the provision of other services carried on using that collateral, provided the firm provides any such service in compliance with any relevant rules, and neither the firm nor any other person takes full title of the assets, and the assets are safeguarded in accordance with CASS. In our final rules, we provide guidance that explains how it should be possible for a firm to provide a staking service for qualifying cryptoassets held as collateral in a cryptoasset borrowing service. We remind firms that providing additional services, such as staking, are dependent on having the correct permissions and complying with the relevant parts of the Handbook.

The situation for non-retail clients is different. The rules in CRYPTO 9, except for the record-keeping requirements and the client reporting requirements, will not apply when the service is provided to non-retail clients. This means that the firm can assume ownership of the collateral when engaging with non-retail clients and utilise practices like Title Transfer Collateral Arrangements (TTCA). When serving retail clients, however, TTCA is explicitly prohibited.

Chapter 7

Safeguarding

Introduction

7.1 This chapter details our final rules for firms that safeguard client cryptoassets. We refer to custody and safeguarding interchangeably in this chapter. It builds on proposals we outlined in DP23/4, then consulted on in CP25/14 and CP26/4. These rules build on our existing client assets regime, which aims to make sure that a firm takes appropriate measures to protect its client assets when they are responsible for them, as set out in CASS. These rules also allow for client assets to be returned as quickly and as whole as possible to clients if the firm enters insolvency.

7.2 The CASS regime supports our statutory objectives and underpins Principle 10 of the Principles for Businesses. This requires firms to arrange adequate protection for client assets when they are responsible for them. Protecting client assets, including client cryptoassets, is fundamental to the trust that consumers place in firms; it is at the heart of ensuring a well-functioning and robust market.

7.3 We have sought to achieve the following outcomes in developing our CASS cryptoasset custody regime, ensuring firms:

- Have adequate arrangements to protect clients' ownership rights to their cryptoassets.
- Have adequate organisational arrangements to minimise risk of loss or diminution of client cryptoassets or the rights in connection with those cryptoassets.
- Maintain accurate books and records of client cryptoassets.
- Have adequate controls and governance to protect client cryptoassets, including the means of access. This can include a private cryptographic key, parts of a private cryptographic key (a shard), or some other means which enables a transfer of the benefit of the cryptoasset to another person.

7.4 In CP25/14, we consulted on CASS rules that would apply in a scenario where a firm was safeguarding client cryptoassets and not carrying on other regulated cryptoasset services.

7.5 In CP25/25, we consulted on cross-cutting requirements which would apply to cryptoasset firms subject to CASS, including the requirement for a PRz, regulatory reporting requirements and client cryptoasset audit requirements. Our final rules for the PRz and regulatory reporting requirements are covered in Chapters 7 and 13 of PS26/13. We will be revisiting audit requirements for all cryptoasset firms in a subsequent consultation and intend to finalise the client cryptoasset audit requirements as part of this work. Our policy intention remains unchanged: that cryptoasset firms subject to CASS will be required to get an audit which checks their compliance with CASS.

7.6 In CP26/4, we consulted on proposed changes to CASS 17 for firms that safeguard client cryptoassets and also carry on other regulated cryptoasset services, such as operating a trading platform, staking, as well as lending and borrowing. Key proposals included:

- The scope and application of our rules for firms offering custody alongside other regulated cryptoasset services.
- Requirements to protect clients' ownership rights through a non-statutory trust in which to hold client cryptoassets, including proposed routes to exit the trust.
- Record-keeping and reconciliation requirements.
- Requirements for private key management and security.
- Requirements for the appointment of third parties involved in cryptoasset custody.

Scope and application of CASS rules

7.7 We proposed to apply CASS 17 to firms meeting the definition of safeguarding created by the Cryptoassets Regulations, and to extend the scope of CASS 17 to custodians of both qualifying cryptoassets and relevant specified investment cryptoassets (RSICs) that provide multiple regulated cryptoasset services. These included:

- Custodial staking, where firms safeguard client cryptoassets and conduct blockchain validation using them, passing back staking rewards to their clients.
- QCATPs or intermediaries safeguarding client cryptoassets.
- Cryptoasset borrowing firms safeguarding client cryptoassets as collateral.

7.8 We also proposed to allow UK CATPs that operate a global settlement float model to move up to 1% of client cryptoassets outside of the trust to facilitate settlement. This limit would be calculated based on cryptoassets safeguarded on trust for each client and by asset type, and subject to the firm obtaining explicit client consent for cryptoassets to be held in this way, with the associated risks clearly outlined.

7.9 In CP26/4, we asked:

Question 27: **Do you agree with our proposed approach to applying CASS 17 in these scenarios? If not, why not, and please describe any scenarios we may not have considered.**

Feedback

7.10 We received 31 responses to this question, of which 48% were supportive, 23% were neutral and 29% were unsupportive.

Application of CASS 17 under Article 9N

7.11 Respondents who supported our approach agreed that applying CASS 17 would strengthen the protection of clients' ownership rights and improve regulatory clarity. These respondents supported extending the CASS regime to the safeguarding elements of services described in CP26/4, including custodial staking, custody provided by QCATPs and intermediaries, and to collateral in cryptoasset borrowing arrangements.

7.12 They agreed that CASS 17 should not apply where a firm does not have control of the means of access to client cryptoassets, for example where clients retain the ability to initiate transfers, and the firm cannot bring about a transfer of the benefit of the cryptoasset.

Application of CASS 17 to different cryptoasset custody models

7.13 Most respondents, including some who were otherwise supportive, sought clarity on how CASS 17 would apply in more complex custody arrangements, where control may be distributed or shared. Examples include multi-party computation (MPC) – a cryptographic method where private keys are split across multiple computer systems, such that no single party can unilaterally transfer the cryptoasset – and overseas third parties, where custody functions may be performed across different jurisdictions. Some respondents raised concerns about operational complexity and the interaction of CASS 17 with existing custody frameworks. Others proposed applying CASS 8 mandate rules for firms that control the means of access for client cryptoassets, rather than CASS 17.

7.14 Among the 29% of respondents who did not support our proposals, several disagreed with applying a trust where clients retain both legal and beneficial title to the cryptoassets (under Article 9N(2)(b)(i) of the Cryptoassets Regulations), or where clients have a right against the firm for the return of the cryptoassets (9N(2)(b)(iii)). Others raised concerns about the feasibility and proportionality of applying a trust in circumstances where a firm controls the means of access but does not hold the cryptoassets itself. More broadly, some questioned the rationale for requiring cryptoassets to be safeguarded on trust in CASS 17, recommending a CASS 6-style outcomes-based approach instead.

7.15 One respondent queried whether CASS 17 should apply to narrow and specialised segments of the market, where firms safeguard cryptoassets subject to statutory powers or court orders.

Application of CASS 17 to custody of RSICs

7.16 Regarding our proposal to apply CASS 17 to RSICs, we received 27 responses on this topic, of which 44% were supportive, 30% were neutral, and 26% were unsupportive. A recurring concern across the feedback was a preference to align our rules more closely with the existing CASS 6 framework, particularly for traditional securities that are tokenised.

Settlement float

7.17 Most respondents broadly supported the exception to hold cryptoassets on trust under the QCATP settlement float model. Some raised concerns that the 1% limit may be too high from a consumer protection perspective, noting that even a small proportion could represent a significant amount of client assets. They emphasised the need for firms to monitor float levels closely and for the FCA to keep the threshold under review. Others felt the proposed 1% limit may be overly rigid, noting that differences in liquidity, trading volumes and market conditions across cryptoassets could make such a fixed threshold too low in practice, particularly during market stress.

7.18 Respondents also raised concerns about applying the limit for each cryptoasset class, suggesting that this may not reflect differences in demand and liquidity and may be difficult to apply where assets are structured in different forms, such as wrapped, bridged or liquid staking tokens.

7.19 Regarding the latter, some respondents also queried whether the staked asset, the liquid staking token, or both, would be considered client cryptoassets due to the different economic rights they represent and their differing functionalities.

Our response

Application of CASS 17, including trust requirements, under Article 9N

We are proceeding with our proposed application of CASS 17, including the exceptions and limitations we consulted on. These exceptions include for cryptoasset lending, for a UK QCATP that uses a settlement float model, where it is necessary for other services, and where the client is indebted to the firm. We have introduced an additional exception detailed further below.

As detailed in Chapter 6, under cryptoasset borrowing arrangements, CASS 17 will also apply to qualifying cryptoasset collateral received from a retail client, including when that collateral is staked.

Outside of the exceptions, in line with the Article 9N definition of safeguarding, CASS 17 will apply to all firms that control cryptoassets through any means that would enable them to bring about a transfer of the benefit of the cryptoassets to another person, whether they themselves hold them or not. The concepts of 'control' and the activity being 'on behalf of another' are our focus, in line with our statutory objectives to protect consumers and maintain market integrity. Self-custody models, where clients safeguard their cryptoassets themselves and firms do not have the ability to bring about a transfer, are not in scope of Article 9N and therefore the CASS rules do not apply. (See also proposed guidance in PERG 19.6.3-19.6.4).

Control can occur from holding or storing of the means of access, or part of the means of access, to the cryptoasset (set out in Article 9N(4)(a) of the Cryptoassets Regulations). Control may also occur from appointing a person to hold or store the means of access, or part of the means of access, to the cryptoasset under an arrangement operated by the firm (set out in Article 9N(4)(b) of the Cryptoassets Regulations). There can also be a combination of both. An example of this is where a person stores part of the means of access but appoints an agent to hold another part under an arrangement which the principal operates. We do not therefore consider there to be a tension for a firm who has the requisite control as defined in Article 9N to meet CASS 17 requirements, including declaring a trust, where they themselves do not hold the cryptoassets or means of access.

We recognise that safeguarding models involving distributed or shared control are common and can provide more robust security arrangements to clients. We do not want to prevent or deter firms from doing so. Rather, we are focused on protecting a cryptoasset owner who may have given control over their cryptoasset to a safeguarding firm. This is because when a safeguarding firm has control of a cryptoasset (as defined in Article 9N of the Cryptoassets Regulations), the underlying technology enables them to carry out actions, including signing transactions, as if they were the owner, whether they have permission from the rightful owner to do so or not.

We acknowledge the feedback challenging the need to impose a trust on firms that carry on the activity outlined in Article 9N(2)(b)(i) in particular – where a client has both legal and beneficial title to the cryptoasset. We did not, however, receive feedback that described business models where this construct exists.

Our concern remains that, should such a business model develop, without requiring the cryptoassets to be safeguarded on trust, there may not be clarity that the client has retained legal and beneficial title to the cryptoassets – particularly where the evidence might show that the client has no control themselves, title to the cryptoasset is not registered (whether to the client or a nominee company), and the conduct between the parties suggests that the firm intends to behave as an owner.

Article 9N(2)(b) enables us to regulate to protect against the harm of uncertainty of ownership in the widest possible range of safeguarding scenarios, in a sector where clients may not always be clear about their ownership rights (and the prevalence of the 'not your keys, not your crypto' ethos).

In terms of advancing our statutory objectives as a regulator, and mindful of the body of case law which has dealt with claims to traditional assets in financial services insolvency through the prism of trusts, we see strong advantages in a Court or Insolvency Practitioner having to approach a dispute (for example in insolvency) from the position that a trust had, as a matter of regulation, been required to protect clients' property rights.

In our final rules we are therefore requiring the creation of a trust to ensure that there is protection for client cryptoassets in insolvency as the UK legal system considers these issues and develops on matters concerning property rights and cryptoassets.

We detail our trust requirements in response to question 28 below. We intend to monitor our policy position on this as the law in this space develops, including whether there may be sufficient legal clarity of clients' ownership rights through other mechanisms in the future. The Law Commission's report on digital assets has considered this to some degree, suggesting that the concept of a control-based legal proprietary interest may develop in this space (although to our knowledge this has not yet occurred).

We also do not consider there to be incompatibility in declaring a trust over cryptoassets subject to court orders or statutory powers, for example in confiscation or similar enforcement proceedings. While the ultimate beneficial owner may depend on the outcome of those proceedings, the trust seeks to ringfence the claims of the client on whose behalf safeguarding is carried on. This client may be an enforcement body that is seizing the assets pending the resolution of legal proceedings, rather than the ultimate beneficiary of those assets (which may itself be determined by those legal proceedings). As in traditional finance custody chains, the party for whom the assets are being safeguarded may not necessarily be the ultimate beneficial owner.

We consulted on the application of CASS 8 to cryptoasset safeguarding firms in CP26/8. We proposed that CASS 8 does not apply to a firm if CASS 17 applies, and that there may be a CASS 8 mandate over cryptoassets (such as a power of attorney held by a discretionary investment manager), but in that context the CASS 8 mandate-holder would not be the safeguarding firm. Rather, the CASS 8 mandate-holder would be in a position to instruct the safeguarding firm. We detail our final rules on the application of CASS 8 in Chapter 5 of PS26/13.

The concept of control for cryptoassets here differs from that of traditional finance custody (and specifically the CASS 8 mandate rules) because CASS 17 applies where a firm has control of cryptoassets within the meaning of Article 9N (that is, the ability to bring about a transfer of benefit of those assets), whereas CASS 8 applies to mandate arrangements where a firm has authority to instruct or direct a client's assets without itself having control. CASS 17 will therefore apply to any cryptoasset firm that has control as defined in Article 9N, subject to the limited exceptions we have outlined.

Application of CASS 17 to different cryptoasset custody models

We recognise that cryptoasset custody arrangements can be complex, where control may be distributed or shared among multiple parties for security reasons. To clarify our position on the application of CASS 17, we have summarised our approach in Diagram 1, recognising the dual concepts of control defined in Article 9N, and based on both existing and hypothetical cryptoasset custody business models. This diagram should be viewed alongside the proposed guidance in PERG 19.6, which clarifies the regulatory perimeter for safeguarding cryptoassets.

To address feedback that applying trust requirements to all parties may be disproportionate under certain custody arrangements, we are introducing another exception to safeguarding client cryptoassets on trust: where a firm holds a back-up key on behalf of a client, and that client retains full control of the cryptoasset and can act independently, whether they are another firm acting as trustee or the owner of the cryptoasset (scenarios 8 and 9 in the diagram). The rationale for this exception, and others, is detailed in response to question 28.

Application of CASS 17 to custody of SICs

We are not proceeding with applying CASS 17 to RSIC custody at this stage. At the outset of the new cryptoasset regime, firms seeking to become authorised to provide RSIC custody will need to do so as a cryptoasset custodian but will need to apply the CASS 6 requirements when safeguarding RSICs for the time being. This includes firms that are currently authorised under Article 40, and if they wish to continue safeguarding RSICs, will need to seek a variation of permission, so their permission includes Article 9N. There may also be firms who are not currently authorised under Article 40 because they are safeguarding, but not safeguarding and administering, RSICs (noting the difference in scope between Articles 40 and 9N). These firms will also need to be authorised under Article 9N (and CASS 6 will apply to that activity, as above).

CASS 6 will also apply to small AIFMs' safeguarding of RSICs where they carry on Article 9N activity, despite the exclusion in Article 72AA of the RAO, just as it does currently in relation to their 'excluded custody activities' (as defined).

Given that CASS 6 rules do not take into account the unique characteristics of RSICs and the feedback we received raised issues with applying CASS 17, we want to engage further on what safeguarding requirements can deliver adequate client asset protection, considering factors such as:

- Whether requirements should differ by type of RSIC.
- How clients' ownership rights can be protected in the absence or nascence of external parties, such as a registrar, central securities depository (CSD) or digital securities depositary that ensures legal ownership of RSICs is accurately recorded and updated.

- How safeguarding frameworks can support fungibility, interoperability and clear accountability as tokenised issuance, trading and post-trade models evolve.

We set out these points in The future of tokenisation: A joint vision and set of regulatory principles for tokenisation in UK wholesale financial markets. This call for input invites industry feedback to inform what CASS rules we may propose to apply to RSIC custody in the longer term.

While firms will be assessed against the applicable CASS 6 requirements when the gateway opens for RSIC custody, we will consult on any further changes to CASS rules once we have engaged further.

RSIC custodians will be subject to finalised non-CASS cryptoasset rules, including relevant sections of COBS, SUP and SM&CR, as these do not depend on the approach in applying CASS.

Settlement float

We are amending our proposal to permit qualifying cryptoasset trading platforms (QCATPs) to hold up to 2% of each client's cryptoassets, calculated per client and per cryptoasset class, outside the trust in a global settlement wallet for settlement purposes. This increase in the limit addresses feedback from some respondents that 1% would not be sufficient to address typical customer trading volumes.

We have clarified that if a client withdraws their consent for cryptoassets to be held in the settlement wallet, firms can no longer use this exemption.

We are not amending the application or approach to calculation of the limit at this stage, for example by introducing a dynamic approach or applying the limit on a portfolio-wide basis. These could result in a materially higher proportion of certain cryptoassets being held outside the trust, without CASS protections, significantly increasing the risk of harm to consumers, especially during periods of market stress when safeguarding protections are most important.

The settlement float is intended to operate as a narrow exception for settlement purposes only, rather than a general liquidity buffer. A defined limit establishes a clear boundary where client cryptoassets may exit the trust, where necessary to facilitate settlement, and supports effective supervision of the exception.

We will monitor our position on the settlement float as the market develops.

Liquid staking

We received feedback asking whether when a firm conducts liquid staking, they must safeguard the staked asset, the liquid staking token or both. Whether the firm safeguards either asset or both will depend on whether the firm continues to have the requisite control to transfer the benefit of the asset and whether they are holding the asset for the benefit of the client. The latter will depend on the specific contractual arrangements of the liquid staking service.

Note: This diagram assumes Firm A is carrying on Article 9N in the UK. It describes Firms B and C as 'Firms' for illustrative purposes only (ie they may or may not need to be authorised, depending on whether they meet the threshold conditions).	Client	Firm A	Firm B	Firm C	Application of CASS 17
1 Client safeguards cryptoasset and private key. **Client has control.** [No Firm has any means that would enable it to bring about a transfer of the benefit of the cryptoasset ie 9N(2)(a)].					N/A
2 Firm A safeguards cryptoasset and private key on behalf of client. **Firm A has control [9N(2)(a)/9N(4)(a)].**					Firm A: all of CASS 17
3 Firm A safeguards cryptoasset and one key shard on behalf of client; Firm B safeguards another key shard on behalf of client. **Firm A has control [9N(2)(a), 9N(4)(a), and 9N(4)(b)] through an arrangement with Firm B.**					Firm A: all of CASS 17 Firm B: N/A
4 Firm A safeguards cryptoasset on behalf of client; Firm A appoints Firm B to safeguard private key on behalf of Firm A to help Firm A strengthen its safeguarding. **Firm A has control [9N(2)(a)/ 9N(4)(b)], Firm B has control [9N(2)(a)/9N(4)(a)]. Firm A is also arranging safeguarding [9N(2)(b)].**					Firm A: all of CASS 17 Firm B: all of CASS 17. Firm A and B are co-trustees.
5 Firm A safeguards cryptoasset on behalf of client; Firm B safeguards a key shard on behalf of Firm A to strengthen its safeguarding; Firm C safeguards on behalf of Firm A to strengthen its safeguarding. **Firm A has control through an arrangement with Firms B and C [9N(2)(a)/9N(4)(b)].** This usually happens within a group.					Firm A: all of CASS 17 Firm B: N/A Firm C: N/A
6 Firm A safeguards cryptoasset on behalf of client; Firm A safeguards one key shard on behalf of client; Firm B safeguards another key shard on behalf of Firm A to strengthen its safeguarding; Firm C is a trusted third party who safeguards back-up key shard on behalf of Firm A in case Firm B fails. **Firm A has control [9N(2)(a)/9N(4)(a)/9N(4)(b)].**					Firm A: all of CASS 17 Firm B: N/A Firm C: N/A
7 Firm A safeguards cryptoasset and one key shard on behalf of client; client safeguards another key shard. Firm B safeguards a back-up key shard on behalf of Firm A to strengthen its safeguarding in case client can't get access (disaster recovery). **Firm A has control through an arrangement with Firm B [9N(2)(a)/9N(4)(a)/9N(4)(b)].**					Firm A: all of CASS 17 Firm B: N/A
8 Firm A safeguards cryptoasset and private key on behalf of client; Firm B safeguards a back-up key on behalf of Firm A to strengthen its safeguarding in case Firm A can't get access (disaster recovery). **Firm A has control [9N(2)(a)/9N(4)(a)/9N(4)(b)]. Firm B has control [9N(2)(a)/9N(4)(a)]. Firm A can step in and take control from Firm B if needed and has contractual dominance over Firm B. Firm A can act independently.**					Firm A: all of CASS 17 Firm B: 17.1, 17.2, 17.4.
9 Client retains private key; Firm A safeguards back-up key shard and through an arrangement, Firms B and C safeguard back-up key shards in case client can't get access (disaster recovery). **Client has control. Firm A has control [9N(2)(a)/9N(4)(a)/9N(4)(b)]. Client can act independently.**					Firm A: 17.4, 17.2. Firms B and C: N/A

Control by any means defined in Article 9N of the Cryptoassets Regulations

Contractual arrangement to provide custody service to the client

This may be the full key or enough shards to execute a transaction

A key shard that cannot on its own execute a transaction

Protecting clients' ownership rights

7.20 In CP25/14, we proposed that client cryptoassets must be segregated under a non-statutory trust to protect clients' ownership rights. We proposed that the terms of the trust could reflect different wallet arrangements, and that firms must maintain records of how the trust is segregated, including the names of clients who are beneficiaries and the relevant cryptoasset class or classes held under the trust.

7.21 In CP26/4, we further proposed that, where necessary to deliver additional services, such as custodial staking, firms could hold an operational surplus of their own cryptoassets within the same trust as client cryptoassets. This surplus would have to be necessary to provide services, made up of the same class as client cryptoassets held in that trust, with firms' claims to it always subordinated to clients' claims, could not be reduced or removed except to remove excesses, be recorded for 5 years after the firm ceased to use it, including the rationale for its use, and subject to the same rules as client cryptoassets held on trust (including on adequate organisational arrangements, record-keeping, means of access and use of third parties).

7.22 In CP26/4, we asked:

Question 28: **Do you agree with our proposed approach to protecting clients' ownership rights, including the approach to the operational surplus and class of cryptoasset? If not, why not?**

Feedback

7.23 We received 28 responses to this question, of which 71% were supportive, 25% were neutral and 4% were unsupportive.

Safeguarding client cryptoassets on trust

7.24 Respondents who were supportive agreed that requiring firms to safeguard client cryptoassets on trust would strengthen clients' ownership rights and improve outcomes in the event of a firm's insolvency. These respondents considered that permitting a limited operational surplus within the trust appropriately recognised operational realities, including staking and settlement-related processes, while maintaining clear segregation between client and firm cryptoassets. Some respondents noted that applying the trust by reference to the class of cryptoasset would support clarity in record-keeping, reconciliations and allocation of shortfalls, and reduce the risk of losses being spread across different cryptoassets.

7.25 Some respondents who were unsupportive raised concerns that requiring client cryptoassets be safeguarded on trust by default may be impractical and disproportionate in certain custody models, particularly where firms do not hold cryptoassets themselves.

7.26 Some noted that trust law is not recognised in all jurisdictions and requiring that third parties acknowledge trusts may prevent firms from safeguarding certain cryptoassets. One respondent noted it would be impossible for a firm to guarantee that no creditor of the firm could claim client cryptoassets, since this will depend on the effect of applicable law.

7.27 Some respondents queried whether and how segregation requirements would apply both with regards to omnibus wallet structures and in arrangements with third parties.

Operational surplus

7.28 Others requested further clarity on the treatment of an operational surplus and the allocation of shortfalls in staking and other protocol-level arrangements. They asked how class of cryptoasset would be assessed, for example whether a wrapped or liquid staking token would be considered a different class to the token it is derived from.

Our response

Safeguarding client cryptoassets on trust

We are proceeding to require firms subject to Article 9N to safeguard client cryptoassets on trust, subject to the exceptions detailed below. While this approach differs from CASS 6, unlike for traditional finance custody assets, there is no external party such as a registrar or CSD to ensure legal ownership is accurately recorded and updated for cryptoassets. Our approach does align with CASS 7, where client money is required to be safeguarded on trust. (Please see our response to question 27 for details on our rationale.)

We have balanced the need to provide firms with sufficient flexibility in drafting the terms of the trust to align with their business models, while establishing a consistent baseline of protection across the market. To help achieve the latter, we will require that the terms and operations of the trust make sure client cryptoassets are not co-mingled with and are separately identifiable to any other assets. This wording is reflected in our rules, instead of referring to segregation, to provide clarity around whether omnibus wallets, for example, will be permitted.

In line with what we consulted on, firms may operate separate trusts through separate virtual addresses or combine client cryptoassets at different virtual addresses into the same trust. Firms will not, however, be permitted to allocate the same single virtual address to different trusts, as this would not meet our co-mingling requirement.

We will require firms to ensure that any appointed third parties for safeguarding keep client cryptoassets separately identifiable to, and not co-mingled with, cryptoassets either belonging to the firm or pertaining to any other appointment. This is to maintain adequate protection of client cryptoassets throughout the safeguarding chain.

We recognise that other jurisdictions may have different legislative frameworks and that there is a risk of harm if a cryptoasset safeguarding firm fails and is subject to an insolvency regime elsewhere that does not afford the same protections as our CASS trust rules. We have addressed this to some extent through our approach to international cryptoasset firms (see FG26/7 and Chapter 2 of PS26/13). Firms that appoint third parties for safeguarding will also be required to consider the jurisdiction as part of their due diligence in concluding that the appointment would not increase the risk of loss of client cryptoassets.

We have amended our guidance on the operation of the trust to address feedback that it may be impossible for a firm to guarantee that no creditor could claim client cryptoassets. We note this will depend on the effect of applicable law, including under any future special insolvency regime that may be available in the UK.

Operational surplus

We are proceeding with our proposal to permit a limited operational surplus within the trust, where it is necessary to deliver additional services. Examples include reduced gas fees from settling transactions, as well as staking, where a firm may need to deposit their own assets in a staking wallet to meet the minimum denomination required to participate in blockchain validation. The surplus will be subject to the same conditions we consulted on, except for requiring the surplus be made up of the same class as client cryptoassets held in that trust.

We have amended this condition to permit a different cryptoasset class for the operational surplus where necessary, whether due to a technical limitation or a feature of the firm's services. This is to accommodate scenarios such as where gas fees from a transaction are paid in a blockchain's native cryptoasset class, which is different to the class of cryptoasset that was transacted (for example, gas fees from a USDC transaction on the Ethereum blockchain are in ETH, rather than USDC).

We will not set a limit on the operational surplus at this stage. This is to take a proportionate approach, providing flexibility depending on the relevant services provided by firms.

Exceptions to the trust

7.29 In CP25/14, we proposed that a firm could remove client cryptoassets from the trust if:

- The firm is providing lending services in relation to those cryptoassets.
- The client instructs a firm to transfer their cryptoassets to another person or to the client themselves.
- It is necessary to use the cryptoassets to discharge a debt owed to the firm as agreed by the client in T&Cs.

- The firm is a UK QCATP operator or the group company of a UK QCATP operator that uses a float model to settle transactions and has obtained the client's informed consent to remove up to 1% of client cryptoassets based on cryptoassets received into the trust for each client and by asset type.
- The firm determines that an absolute transfer of title and ownership from the client to the firm or another person is necessary to deliver the product or service and has obtained the client's informed consent.

7.30 In such cases, the cryptoassets would cease to be treated as client cryptoassets and would no longer benefit from CASS protections.

7.31 In obtaining clients' consent, we proposed that firms must explain the risks to clients of their cryptoassets not being held on trust, including if the firm fails, and for retail market business, this process must be compatible with the Consumer Duty. The record of this consent would have to be kept for a period of 5 years after the firm stops relying on it to exempt client cryptoassets from the trust.

7.32 In CP26/4, we asked:

Question 29: **Do you agree with our proposed approach to exempting firms from holding cryptoassets on trust in certain scenarios? If not, why not?**

Feedback

7.33 We received 27 responses to this question, of which 67% were supportive, 26% were neutral, and 7% were unsupportive.

7.34 Respondents who were supportive agreed that providing targeted exceptions from holding cryptoassets on trust was appropriate where a trust-based model would be impractical or disproportionate.

7.35 Some respondents who were unsupportive raised concerns that permitting cryptoassets to move in and out of the trust could weaken clients' ownership rights and increase the risk that clients may not clearly understand whether their cryptoassets benefit from CASS protections at a given point in time and that client consent and disclosures may not be sufficient. Some respondents thought that the proposed exceptions may be difficult to apply consistently across complex or hybrid custody models.

7.36 A few respondents questioned whether requiring a trust was the appropriate starting point given the number of exceptions already deemed necessary to enable firms to provide services. Others noted that the approach could unduly restrict innovation as market practices develop and additional scenarios warranting further exceptions may arise over time.

7.37 Some respondents requested further clarity on how firms should determine that an exception is appropriate, and whether certain activities, such as discretionary dealing mandates, would be permitted.

Our response

We are proceeding with the permitted exceptions to the trust that we consulted on. While these exceptions reduce CASS protections, they do not weaken the rationale for, or appropriateness of, our trust requirements. Rather, they seek to accommodate the realities of a fast-evolving market. Equally, clear and proportionate safeguards can support innovation by providing greater confidence in the regulatory framework to firms and consumers. We will continue to monitor both our trust requirements, and permitted exceptions, as market practices develop.

We are also introducing an additional exception to the trust rules for the situation where a firm holds a back-up key on behalf of a client, but that client retains full control of the cryptoasset and can act independently. This exception will apply both when the client is the cryptoasset owner themselves and when the client is itself another safeguarding firm acting as trustee for its own clients. This is proportionate to the risks of harm, as the primary advantage of a trust is that it protects clients from competing claims to their cryptoassets in insolvency. If the firm that holds a back-up key enters insolvency, either the owner themselves continues to retain full control of their cryptoassets (and so would not need to rely on an insolvency process for the return of their cryptoassets) or the owner will be protected by the safeguarding firm, acting as trustee, which appointed the failed firm.

While there are still risks of harm in this scenario – for example, misuse or theft of the cryptoassets by virtue of the firm having a back-up key – these firms will remain subject to CASS 17.2 and 17.4. They also will not be permitted to appoint third parties (CASS 17.6). This is to mitigate further associated risks of harm, for example if the third party has weak or inadequate systems and controls or conducts fraud.

We are not seeking to restrict firms from having discretionary dealing mandates for cryptoassets. Rather, CASS 17.3.9 explicitly notes that for such services, firms may be able to rely on the exception from acting as a trustee under CASS 17.3.6, if the conditions in that rule are met. These conditions are that the firm is providing a service to clients where it is necessary for the firm to have ownership of the cryptoasset; and/or to effect a transfer of ownership of the cryptoasset to another person; and the firm has obtained the client's prior informed consent.

Record-keeping

7.38 In CP25/14, we proposed that firms must maintain client specific records which would enable them to identify, for each client, the type, quantity and location of cryptoassets held, the nature of the client's claim to those cryptoassets, and any other persons with the capacity or control to effect a transfer. We proposed that firms must maintain these records independently from the relevant distributed ledger technology (DLT) used, and that firms cannot rely on records kept by third parties.

7.39 In CP26/4, we further proposed that the CASS record-keeping rules (CASS 17.5) only apply to firms safeguarding client cryptoassets as trustee. Cryptoassets held outside the trust (including where the client has a contractual right of return) would no longer be considered client cryptoassets. Other record-keeping rules may apply, depending on the firms' other regulated activities (eg CRYPTO 9.4 for cryptoasset lending and borrowing and CRYPTO 10.5 for staking firms.) The CASS trust record would have to be kept for a period of 5 years after the relevant trust has been brought to an end.

7.40 We also proposed to permit firms not to include the actual name of the third party or person with the capacity to effect a transfer where doing so would compromise the firm's ability to protect client cryptoassets, provided that the record contains sufficient information to identify that person using the firm's other records.

7.41 In CP26/4, we asked:

Question 30: **Do you agree with our proposed approach to record-keeping requirements, including only applying them to client cryptoassets held on trust? Please explain your answer and indicate whether this approach would create a gap in consumer protection.**

Feedback

7.42 We received 30 responses to this question, of which 63% were supportive, 30% were neutral, and 7% were unsupportive.

7.43 Respondents who were supportive agreed that limiting record-keeping requirements to client cryptoassets held on trust was proportionate. They considered that requiring firms to maintain independent, accurate and up-to-date records would support effective reconciliations and supervisory oversight.

7.44 Some respondents who were unsupportive raised concerns that limiting record-keeping requirements to cryptoassets held on trust could create gaps in consumer protection where clients retain exposure to cryptoassets held outside the trust. Concerns were also raised that the requirement for records to be accurate 'at all times' was impractical in continuously operating markets. Some respondents were concerned about maintaining records independently from the DLT, noting that on-chain records provide immutable evidence of balances and transaction flows.

7.45 Some respondents requested clearer identification standards for record-keeping requirements, noting that asset names alone may not be sufficient where multiple tokens share similar identifiers. They suggested using more standardised identifiers, such as the Digital Token Identifier (DTI), to avoid ambiguity.

Our response

We are proceeding with the requirements that firms safeguarding client cryptoassets as trustee must keep records that enable them to identify for each client the type, quantity and location of cryptoassets held, and any other persons with the capacity or control to effect a transfer.

Cryptoassets safeguarded outside of the trust will not be subject to CASS record-keeping requirements, as they would no longer be considered client cryptoassets and would be subject to other relevant record-keeping requirements (for example, for staking, or lending and borrowing).

Feedback suggested we were not sufficiently clear about our policy intentions with regards to the use of DLT. Our final rules confirm that firms will be permitted to use DLT as an external source of information to confirm the per-trust/class cryptoasset resource (ie the amount and class of cryptoasset they are safeguarding on trust for clients), where they have not appointed third parties for safeguarding.

However, the same source of information cannot be used to calculate the per-trust/client/class cryptoasset requirement. This is because the requirement calculates what firms *should* be safeguarding; the resource confirms what firms are safeguarding (for example in their trust wallets). Crucially, maintaining independent sources of information ensures that reconciliations are effective in identifying discrepancies.

This independence must also be maintained where a firm appoints a third party to safeguard client cryptoassets on trust. This means that the resource confirmation in this scenario must come from information provided by the third party rather than relying on the DLT. Otherwise, the third party's confirmation of the resource will not effectively identify discrepancies if it relies on the same source as the one used by the firm to calculate the requirement (the DLT).

We have removed references to records being accurate 'at all times', to take a proportionate approach, noting that reconciliations will be required per business day (please see our final rules below). Our expectation remains that firms must maintain accurate records to ensure client cryptoassets are adequately protected at all times.

In response to feedback on standardised identifiers, we have introduced a new defined term for '*safeguarding cryptoasset class*' which is blockchain sensitive and allows reference to digital token identifiers where relevant. This means that a firm safeguarding client cryptoassets would need client agreement in order to return an equivalent asset to their client via a different blockchain than the one on which the safeguarding arrangement began.

Reconciliations, addressing shortfalls and excesses

7.46 In CP25/14, we proposed a reconciliation framework to ensure firms test the accuracy of their records and identify and resolve shortfalls in the amount of client cryptoasset holdings.

7.47 In CP26/4, we further proposed that firms:

- Perform daily reconciliations to calculate, for each client and trust they operate, the amount of each cryptoasset class they are required to safeguard and to confirm the amount of client cryptoassets they are safeguarding.
- Take appropriate action where discrepancies are identified, including removing any excess cryptoassets from a trust unless they form part of a permitted operational surplus, and topping up any shortfalls in the relevant cryptoasset class using their own resources or by procuring a third party to do so.
- Notify the FCA if a shortfall had not been topped up by the next reconciliation, including the reasons for the shortfall and the impact on clients; the firm's approach to notifying clients; if the firm's internal records are materially out of date, inaccurate or invalid; or the firm is unable or materially fails to comply with the reconciliation requirements.
- Determine whether to notify affected clients about a shortfall, including reviewing that decision at least once a day until the shortfall is resolved.

7.48 In CP26/4, we asked:

Question 31: **Do you agree with our proposed approach to reconciliations, topping up shortfalls and removing excesses? If not, why not?**

Feedback

7.49 We received 37 responses to this question, of which 32% were supportive, 43% were neutral, and 24% were unsupportive.

7.50 Respondents who were supportive agreed that requiring firms to conduct reconciliations would support the timely identification of discrepancies and strengthen safeguarding outcomes. They considered that reconciliations on a per-trust, per-client and per-cryptoasset class basis would help protect client cryptoassets, with some noting that organising assets by cryptoasset class could also provide clarity in the allocation of shortfalls.

7.51 Respondents also noted that requiring firms to top up shortfalls promptly using their own resources would help reduce the risk of consumer harm and maintain confidence in custody arrangements, and that notification and escalation requirements were appropriate to support supervisory oversight.

7.52 Some respondents who were unsupportive raised concerns that the requirements for resolving discrepancies were more restrictive than in CASS 6. Some expressed concerns about the requirement to top up shortfalls using cryptoassets of the same class, noting that this could be challenging, particularly for less liquid assets. They also raised concerns that requiring them to notify the FCA of all unresolved shortfalls, regardless of size or cause, could be burdensome. They requested a distinction between shortfalls due to timing mismatches, network congestion or protocol-level delays, and those that pose risks to redemption.

7.53 Some respondents emphasised that a shortfall in client cryptoassets is a serious event and raised concerns about the level of discretion afforded to firms in deciding whether and when to notify clients.

7.54 Respondents also requested further clarity on how the reconciliation requirements would operate across more complex custody arrangements, including multi-wallet, multi-chain and third-party models.

Our response

We are proceeding with our reconciliation requirements that firms must investigate discrepancies, remove all excesses, top up any shortfalls and notify the FCA in writing if a shortfall has not been topped up by the next reconciliation. Noting feedback highlighting the impact of shortfalls on consumers and the importance of transparency, we will require firms to immediately notify clients affected by shortfalls.

We do not distinguish between treatment of shortfalls based on their cause. Shortfalls for the purposes of CASS 17 rules will occur where the firm's per-trust/class cryptoasset resource is less than the total per-trust/client/class cryptoasset requirement and must be topped up.

While CASS 7 and 15 provide flexibility for firms in resolving discrepancies arising from timing differences between accounting systems, these relate to discrepancies in firms' external reconciliations, rather than shortfalls in client assets. External reconciliations in CASS 7 and 15 involve comparing the balances in firms' internal records to those of third parties, such as banks where client money or safeguarded funds have been deposited. Timing differences can therefore occur from banks

setting cut-off periods for their reconciliations, based on when traditional finance markets close. This is not applicable in cryptoasset custody, given the 24/7 nature of the market, and the approach to reconciliation differs in CASS 17.

We are proceeding with our requirement that shortfalls must be resolved in the relevant class of cryptoassets. While this differs from the approach in CASS 6, it is proportionate and seeks to mitigate the risk of loss of client cryptoassets, noting the flexibility and exceptions to the trust afforded to firms in CASS 17.

To address feedback on the challenges in resolving shortfalls for illiquid cryptoassets, we have clarified that firms may choose to set aside or transfer an alternative asset of the same value to affected clients in such instances. Firms can then agree with their clients that they no longer need to safeguard the relevant cryptoassets in shortfall for them, which would then need to be reflected in the calculation of what they should be safeguarding. If clients do not agree to this, firms will still need to top up the shortfall in the relevant class of cryptoassets. For retail clients, firms would need to act compatibly with the Consumer Duty – for example, considering fair value, consumer understanding and consumer support.

Private key management and security

7.55 In CP25/14, we proposed a technology-agnostic and outcomes-based approach to private key management and security, recognising the rapidly evolving nature of custody technologies. We proposed that firms must maintain adequate organisational arrangements to ensure the secure generation, storage and control of the means of access to cryptoassets throughout their lifecycle. These measures are consistent with our approach to applying the operational resilience framework in SYSC 15A to cryptoasset firms (see Chapter 8 of PS26/13).

7.56 Means of access is defined as a private cryptographic key, parts of a private cryptographic key or some other means which a person would need possession or knowledge of to bring about a transfer of the benefit of a cryptoasset to another person. This could include cold wallets and hardware security modules, as well as hot wallets.

7.57 We proposed that firms must maintain accurate and up-to-date records explaining how control is exercised, for example where sharded keys or similar arrangements are used. Arrangements would need to include appropriate measures to mitigate the risk of loss or compromise of the means of access, including effective back-up and recovery processes.

7.58 In CP26/4, we further proposed that these requirements would apply to client cryptoassets safeguarded as trustee, including any permitted operational surplus. We also proposed that firms must maintain a means of access record which explains how a firm holding shards exercises control, which is reviewed at least once each business day.

7.59 In CP26/4, we asked:

Question 32: **Do you agree with our proposed approach to private key management and security? If not, why not?**

Feedback

7.60 We received 34 responses to this question, of which 44% were supportive, 50% were neutral, and 6% were unsupportive.

7.61 Respondents who were supportive agreed that adopting a technology-agnostic and outcomes-based framework was appropriate given the pace of change in cryptoasset custody technologies. They noted that requiring firms to maintain accurate and verifiable records explaining how control over cryptoassets is exercised would support effective supervision and strengthen safeguarding outcomes. They agreed that limiting the application of these requirements to client cryptoassets safeguarded as trustee, including any operational surplus held under trust, was proportionate to the risks.

7.62 They noted the requirement to implement measures to mitigate the loss or compromise of the means of access, including secure back-up arrangements, was appropriate given the irreversible nature of cryptoasset transactions.

7.63 Some respondents sought clarity on what constitutes the 'means of access', particularly in more complex arrangements such as sharding, where a private key is divided into distinct shards or segments that must be re-combined to sign transactions or MPC, a zero-knowledge method where transactions are signed by parties holding valid key shards, without the private key ever recombining.

7.64 Others noted the need for clearer supervisory expectations around how firms should evidence control in complex key management arrangements. They also suggested greater emphasis on the testing and assurance of back-up and recovery processes to ensure these controls operate effectively.

7.65 Some raised concerns about dependency risk where third parties form part of the key management chain, noting that clearer expectations around monitoring, contingency planning and supervisory visibility would improve resilience. Some feedback suggested that a clearer link between key compromise events and prompt regulatory escalation would support early intervention and consumer protection.

7.66 Some feedback the consumer protection benefits of the daily review of the means of access record, given the significant consequences if the means of access were lost or compromised. Others requested clarity on the rationale and purpose of the review. They highlighted that it may be impractical, particularly where control arrangements do not change frequently, and could inadvertently increase the risk of fraud or theft, particularly for hardware security modules (HSM) or hardware wallets, where the review may require physical checks. In some cases, more frequent access to sensitive credentials may increase the risk of compromise.

7.67 Others raised concerns that applying the requirements to validation or signing keys used for staking could be disproportionate.

Our response

Scope and application of CASS 17.4

We are proceeding with most of our means of access rules as consulted on. To clarify, these rules will apply to means of access, which is defined as a private cryptographic key, parts of a private cryptographic key, or some other means which a person would need possession or knowledge of to bring about a transfer of the benefit of a cryptoasset to another person. This could include cold wallets and hardware security modules, as well as hot wallets. These rules seek to ensure the means of access are protected against the risks of inoperability, inaccessibility, loss, fraud and irrecoverability.

We recognise that these rules go beyond what CASS has traditionally covered. This is by design, to reflect the important role of cryptoasset custodians in protecting private keys, the function of private keys in exercising control, and the generally irreversible, immutable nature of cryptoasset transactions.

We are amending the application of CASS 17.4 to include firms that are providing a back-up solution, alongside those that are safeguarding client cryptoassets on trust. This is to take a proportionate approach, reflecting the complexity of custody arrangements highlighted in the feedback, and the additional exception to the trust we have introduced (see CASS 17.3.12).

We are not providing further targeted guidance on supervisory expectations relating to private key management at this stage. We want to provide flexibility in how firms comply with CASS 17.4, suited to their business models, noting the complexity of private key arrangements across the market. We will review our approach, including whether to set minimum supervisory expectations, as the market develops.

The application of the means of access rules to staking 'validator' and 'withdrawal' keys will depend on whether they can be used to transfer the benefit of a cryptoasset on behalf of another (as per the definition of safeguarding in the Cryptoassets Regulations). We do not expect this to be the case for keys used solely for enabling blockchain validation in staking, but may occur for 'withdrawal' keys, depending on the business model.

Means of access record

To remain proportionate, technology agnostic and flexible to firms' specific arrangements, we are not proceeding with the requirement that firms must review each client's means of access record at least once each business day. We will continue to require that firms must promptly update the record as often as necessary for the details within them to remain accurate. This may include but is not limited to monitoring arrangements that reflect the continuous nature of markets firms operate in.

Dependency risk
We have included in guidance that in establishing robust security and organisational arrangements, firms should also consider dependency risk, ie where they are dependent on others to carry out their safeguarding responsibilities. This could occur from distributing the means of access among too many staff members or devices or relying too much on other firms to exercise control of client cryptoassets.

Appointment of third parties

7.68 In CP25/14, we proposed that firms could appoint third parties in cryptoasset custody, where this was necessary for safeguarding and in the client's best interests, supported by appropriate due diligence, trust protections and contractual arrangements.

7.69 In CP26/4, we further proposed that the requirements on appointing third parties would apply only where cryptoassets are safeguarded on trust. We also proposed to refine the standard for appointing third parties. Rather than requiring that such appointments be necessary for safeguarding and in the client's best interests, firms would be required to make sure that any appointment would not increase the risk of loss or diminution of client cryptoassets. This assessment would be supported by the firm's due diligence and organisational arrangements, and firms would be required to evidence it in a written policy on a case-by-case basis.

7.70 In the context of safeguarding chains, where an appointed third party uses another third party, we proposed that firms may rely on their appointee to conduct due diligence on the subsequent third party and report its findings.

7.71 Finally, we proposed that firms may delegate Board approval for the appointment of a third party to the person performing the prescribed responsibility (PRz) for safeguarding under the Senior Managers & Certification Regime (SM&CR), or to a committee including that individual.

7.72 In CP26/4, we asked:

Question 33: **Do you agree with our proposed approach to the use of third parties? If not, why not?**

Feedback

7.73 We received 37 responses to this question, of which 51% were supportive, 46% were neutral, and 3% were unsupportive.

7.74 Respondents who were supportive agreed that permitting firms to appoint third parties to safeguard client cryptoassets, subject to appropriate conditions, reflected operational realities and existing custody models. They considered that due diligence, oversight and governance requirements for third-party appointments would support effective safeguarding and mitigate risks of harm. Respondents further noted that clarifying firms' ongoing responsibility for compliance with CASS 17, even where third parties are used, was appropriate and consistent with existing CASS principles. The move away from requiring that third-party appointments be necessary for safeguarding was welcomed.

7.75 Some respondents who did not support the proposal raised concerns that the scope of the requirements may not be sufficiently clear in more complex custody arrangements, with multiple third parties and particularly where providers do not have control over the means of access. Others raised concerns that prohibiting set-off or similar rights over client cryptoassets could limit commercial flexibility in certain institutional arrangements.

7.76 Some respondents requested additional guidance on how the rules would be applied alongside outsourcing and operational resilience requirements. Others queried how cross-border arrangements could work, both in terms of protecting clients' ownership rights, and for firms conducting due diligence, for example on third parties operating in jurisdictions with more principles-based safeguarding regimes.

Our response

We are proceeding with our requirements for firms that appoint third parties to safeguard client cryptoassets. These requirements apply as well as the SYSC outsourcing and oversight framework.

SYSC 8 defines outsourcing as 'an arrangement of any form between a firm and a service provider by which that service provider performs a process, a service or an activity which would otherwise be undertaken by the firm itself'. This could include, but is not restricted to, custody infrastructure such as MPC and HSM providers. Other examples of outsourcing requirements include third-party node operators and transaction signing infrastructure (please see FG26/6 for more guidance on cryptoasset operational resilience).

The rules for appointing third parties to safeguard will apply to all firms that are safeguarding client cryptoassets on trust.

We have clarified in guidance that firms may appoint third parties in jurisdictions with regulatory requirements for cryptoasset safeguarding that use different terms, while covering the same aspects of financial and operational resilience, security of the means of access, and record-keeping.

Our final rules do not permit firms to grant a security interest, lien or right of set-off to third parties, as we do not consider this compatible with ensuring appointing third parties does not increase the risk of loss or diminution to client cryptoassets. We will consider whether a change in approach may be warranted in the future, depending on market developments (other than specified investment cryptoassets, which are currently excluded from the scope of CASS 17 rules).

Firms providing back-up solutions that have applied an exception to the trust under CASS 17.3.12 will not be permitted to appoint third parties. This is to mitigate further associated risks of harm, for example if the third party has weak or inadequate systems and controls, or conducts fraud, noting the back-up provider firms in this scenario will not be acting as trustee.

Chapter 8

Staking

8.1 This chapter sets out the feedback to our proposed requirements – with a focus on promoting more robust consumer understanding of staking – for firms engaged in arranging qualifying cryptoasset staking (authorised cryptoasset firms), as defined in the Cryptoassets Regulations. Staking is an industry term which refers to the practice of locking up cryptoassets to help secure and validate transactions on a blockchain network in return for a reward.

8.2 Our analysis has indicated that retail clients may have a limited understanding of the underlying technological process of staking and may conflate this activity with other reward generating services such as cryptoasset lending and borrowing. They are often not aware that cryptoassets may need to be locked-up for a period of time in order to participate in blockchain validation as part of the proof-of-stake consensus mechanism. Retail clients may also not understand that financial rewards are generated and distributed from the blockchain network, typically based on newly issued cryptoassets from blockchain validation and a share of blockchain transaction fees, which acts as an incentive for contribution of cryptoassets to the staking process.

Consumer Understanding

Consultation proposals

8.3 In CP25/40 we consulted on requirements seeking to strengthen retail clients' understanding of the staking activity including its nature, features and risks, before they are engaged in the activity.

8.4 These proposed requirements, only applicable to staking services provided to retail clients, include requiring authorised cryptoasset firms to:

a. Give information about the firm and its staking service before providing a staking service, to support retail clients' understanding.

b. Provide the key terms of agreement for the staking service (which form part of the contract) and obtain the clients' express consent in relation to those terms prior to the commencement of the service each time a retail client instructs a firm to provide a staking service.

8.5 We specified the information firms must cover in key terms, including fees, rewards, and duration of staking (ie retail clients may not be able retrieve their cryptoassets in a timely manner) (see CRYPTO 10 for the final list of points to be covered in key terms).

8.6 We proposed that the requirements at (b) above had to be met each time a retail client instructs a firm to provide a staking service. We also separately proposed that authorised cryptoasset firms must notify clients in good time of material changes

to any of the information and/or key terms provided to clients, in addition to the requirements at (b).

8.7 In CP25/40, we asked:

Question 25: **Do you agree with our proposal that regulated staking firms must provide retail clients with information on the firm and its staking service, and provide the key terms of agreement in relation to those services and obtain retail clients' express prior consent in relation to those terms each time cryptoassets are staked, as outlined in paragraphs 6.14-6.19? If not, please explain why not?**

Question 26: **Do you agree that our proposed information provision, key terms and express prior consent requirements should only apply to retail clients and not to non-retail clients? If not, please explain why not?**

Feedback

8.8 Most respondents (81%) supported our proposals to require authorised cryptoasset firms to provide retail clients with information on staking and obtain their consent to stake cryptoassets. They highlighted that many retail clients lack a basic understanding of staking processes, validator risks, and the implications of locking up cryptoassets. Some staking firms and industry associations welcomed that our proposals do not prescribe a specific format or template.

8.9 A majority of respondents (83%) supported our proposal that consumer understanding requirements should apply only to retail clients, as they are more likely to have insufficient knowledge of staking. A small number of respondents considered that consent and disclosure should extend to non-retail clients or small businesses, claiming this would not significantly increase burden on firms while offering further protection.

8.10 However, some respondents (25%), mostly firms actively offering staking services, were concerned that our rules may only allow staking firms to obtain single-instance consent to stake specified amounts of cryptoassets. They suggested that only allowing firms to obtain consent on this basis could cause "consent fatigue" and reduce retail clients' engagement with information on staking. Some respondents added that our proposed rules would prevent firms from continuing to offer popular 'auto staking' models, where clients authorise firms to automatically stake current and future holdings of eligible cryptoassets which the client is safeguarding with the firm. Only 2 respondents explicitly supported requiring information provision and consent requirements to be met for each separate instance of cryptoasset staking.

8.11 A few respondents recommended minor amendments or clarification on the information points that staking firms must provide to retail clients. They noted that the draft rules appear to assume staking always involves a transfer of ownership or that

cryptoassets are always locked and inaccessible during staking – neither of which applies across all staking models.

8.12 Some respondents also sought clarifications on the perimeter of the regulated activity of arranging staking, and its interaction with different business models (eg non-custodial and liquid staking) or with the staking process (eg infrastructure supporting blockchain validation).

Our response

We have considered the feedback on our consumer understanding proposals carefully. In light of the majority support and recognition that our overall approach could support better consumer understanding, we will proceed with our overarching proposal that, before commencement of a staking service, authorised cryptoasset firms must:

a. Give retail clients information on the firm and its services, including risks (such as slashing or other operational disruptions).

b. Provide the key terms of the service (which form part of the contract) and obtain the retail clients' express prior consent in relation to those terms.

These requirements will only apply to services involving retail clients and need to be met either before clients enter into a staking contract, or prior to their cryptoassets being staked.

We have also considered feedback on the frequency of the requirement for firms to provide information and obtain consent – particularly whether the information should be provided by the firm to clients prior to each separate instance of staking, and how these requirements would impact retail clients' protection and firms' operations.

Under our final rules, firms will not be required to provide information and obtain consent prior to each, separate instance of staking retail clients' cryptoassets.

We have considered further how different business models operate (including the risks they could pose) and how best to support retail clients' understanding of the services that they engage with. We have considered the risks of auto-staking and are ensuring the final disclosure and consent rules enable firms to continue offering these types of services. This will help maintain a broad range of services for retail clients, and support competition in the staking market.

Staking firms, under the final rules, can obtain consent from retail clients to stake the retail client's existing and future holdings of a specific type of cryptoasset or multiple specific cryptoassets. Staking firms are not required to obtain consent each-time prior to each, separate instance of staking cryptoassets. Our rules, however, do not permit firms to obtain blanket consent from retail clients to stake either current or future holdings of any, unspecified, cryptoassets. This approach reflects that there may be differences in the characteristics of staking different types of cryptoassets,

including in the time needed to begin and cease staking, and that retail clients should consent only to the staking of specified cryptoassets. The key terms of the service must be provided to retail clients.

We are also introducing additional requirements to mitigate any heightened risk of reduced client engagement with information when retail clients use auto-staking services. For auto-staking, the terms of agreement must state that the firm may stake a client's future holdings of a specific cryptoasset and, additionally, how the service can be cancelled. The staking firm must also obtain the retail client's express prior consent to the terms of this agreement. For all staking service models, firms will also be required, at least every 12 months after the original consent was obtained, to notify retail clients of the staking service which they are using. This includes the amount of cryptoassets currently being staked for the client, total rewards earned as part of the staking service, total fees and commission charged, and the most recent terms of service.

We are introducing guidance provisions on scenarios in which it may be in the best interests of a retail client for the firm to provide the above notification sooner than 12 months after the original consent to stake cryptoassets was obtained. Examples includes where the client has not accessed the platform through which staking is provided for a significant period of time.

In addition to this notification requirement, our rules still require staking firms to notify retail clients of material changes to key terms in good time, including with respect to fees or duration for which cryptoassets will be locked up. Firms should consider the Consumer Duty and consumer rights law, amongst other applicable legal principles, rules and guidance, when making any variations to key terms.

When preparing information on staking for retail clients, firms should bear in mind that clients may not understand the technical mechanics of staking or the relevant terminology. Firms should, however, aim to help clients understand a staking service's economic nature and consequences for the client.

We note that staking firms are subject to financial promotions requirements and must comply with the Consumer Duty. Firms should consider whether, beyond what is required by the staking rules, providing additional information to retail clients could improve understanding. Further guidance on the Duty, including examples of its application to cryptoasset staking, can be found in PS26/13.

We note the feedback we received seeking clarity on the types of information provided to retail clients. With regard to suggestions that firms should be required to explain that staking rewards earning is protocol driven, rather than determined by a firm, we note that our rules already require key terms to state how staking rewards are determined and whether they are variable. We recognise that transfer of cryptoasset

ownership or the locking up of cryptoassets are not features of all staking services. The rules consulted on in CP 25/40 cater for this reality, and we have therefore not made amendments to rules or guidance on this point.

When providing information on what are commonly known as "liquid staking services", firms should be clear with the clients on the impact of transfers of liquid staking tokens. We have clarified in our rules that key terms must include information on the type, amount, and associated rights and obligations of any cryptoassets issued to a retail client as part of a staking service.

Record keeping

Consultation proposals

8.13 We consulted on the proposal to require authorised cryptoasset firms to maintain certain records of services provided to both retail and non-retail clients. We specified that where a client who was issued a liquid staking token transfers the token to another person, the firm should maintain the records of the transfer. These records must be maintained for 5 years from the point at which the record is created.

8.14 In CP25/40, we asked:

Question 27: **Do you agree with our proposed record-keeping requirements on regulated staking firms? If not, please explain why not?**

Feedback

8.15 83% of respondents supported our proposed record-keeping requirements. Respondents noted that strong record-keeping is essential for consumer protection and regulatory oversight, ensuring firms can evidence client instructions and provide staking services in line with the agreed terms, including correct distribution of staking rewards. Respondents also agreed that a 5-year retention period for records was appropriate and aligned with broader regulatory standards.

8.16 Several respondents (10%) suggested that there may be challenges in firms meeting these requirements in the case of liquid staking models, as they may not necessarily have information on a liquid staking token holder's identity. Several respondents queried to what extent firms could rely on on-chain blockchain data to meet record-keeping requirements.

Our response

We will proceed with our proposed record-keeping requirements on authorised cryptoasset firms. This includes the proposed 5 year-retention period for these records, albeit with some exceptions where certain records must now be maintained for the duration of the client relationship where this exceeds 5 years. Our approach to record-keeping requirements aligns with the stakeholder feedback received, allows for proportionate regulatory oversight and in turn supports consumer protection.

We have carefully considered comments that firms maintain certain records of staking services, such as total rewards allocated to each client, on a per day basis. We consider that this approach is feasible and proportionate to ensuring firms provide staking services appropriately under the agreed terms, and it is consistent with our overall record keeping approach.

We recognise that in some liquid staking models, the original client who was issued a liquid staking token may transfer it to another person without the staking firm knowing that other person's identity. Liquid staking rewards are generally distributed through 2 models. In the 'reward-bearing' model, the token's value increases relative to the underlying cryptoasset and rewards are realised only when the token is exchanged. In the 'rebasing' model, wallets holding liquid staking tokens are automatically credited with additional liquid staking tokens as rewards accrue. In both models, if a token is transferred, firms do not need to know the natural identity of the token holder for the holder to be able to receive staking rewards.

We have amended requirements so that firms are only required to keep records in respect of clients whose identity is known to the firm. This ensures that staking firms maintain the records needed to demonstrate that they are providing staking services in accordance with the agreed terms, while avoiding any requirement to maintain records in respect of subsequent transferees of liquid staking tokens beyond the client whose identities the firm is unlikely to be able to ascertain. To ensure that firms maintain appropriate records in liquid staking models, we have amended our rules to require staking firms to keep records of the type and amount of any cryptoassets provided to clients as part of a cryptoasset staking service.

Staking firms should note that where cryptoasset safeguarding also takes place, CASS 17 requirements on safeguarding record keeping will apply (see Chapter 7 of PS26/11).

Lastly, we want to note that our current staking requirements have not prescribed which specific methods (including on or off-chain) firms may use to implement record keeping requirements.

Chapter 9

Decentralised Finance (DeFi)

9.1 This chapter sets out the feedback to our proposed requirements for firms engaging in decentralised finance (DeFi).

DeFi guidance

9.2 In CP25/40 we proposed to apply rules and guidance to firms engaging in DeFi where there is a clear controlling person(s) carrying on one or more of the new cryptoasset activities defined in the Cryptoassets Regulations. This follows the approach in the Treasury's policy note, which stated that 'where specified activities are being undertaken on a truly decentralised basis, ie where there is no person that could be seen to be undertaking the activity by way of business', then they would not fall in scope of the regulated activities. As we outlined in CP26/13 (cryptoasset perimeter guidance consultation), whether a person is in scope of a regulated activity will be assessed on a case-by-case basis.

9.3 We also proposed to separately consult on DeFi guidance later this year. The proposed guidance seeks to cover indicators of degrees of (de)centralisation, and how proposed requirements and guidance for regulated cryptoasset activities would interact with firms engaging in DeFi. It will also give guidance on how to mitigate operational resilience and financial crime risks when integrating or interacting with DeFi.

Consultation proposals

9.4 In CP25/40, we asked:

Question 28: **Do you agree with our proposal to apply rules and guidance in CP25/40 Chapters 2-6 and guidance to firms engaging in DeFi where there is a clear controlling person(s) carrying on one or more of the new cryptoasset activities? If not, please explain why not?**

Feedback

9.5 The majority of respondents (91%) expressed strong support for applying the rules and guidance where a clear controlling person undertakes one or more of the new cryptoasset activities. These respondents generally recognised the principle of 'same risk, same regulatory outcome'. They also agreed on the importance of preventing regulatory arbitrage, specifically by firms acting as intermediaries in substance while presenting themselves as decentralised. They added that persons exercising material influence over protocol design, operation or user assets should be subject to appropriate regulatory oversight.

9.6 These respondents also supported the need to consult on separate DeFi guidance and welcomed continued engagement with us. Respondents agreed the forthcoming guidance should provide clear and objective indicators of de(centralisation). Some respondents (24%) shared that indicators could focus on established concepts of financial intermediation. For example, safeguarding of client cryptoassets, exercising discretion over execution or settlement, or maintaining account relationships, rather than technical proximity to a protocol or its governance structure.

9.7 A minority of respondents (9%) suggested taking a more bespoke approach to DeFi in guidance, emphasising that any high-level indicators might create barriers to implementation and in turn stifle innovation.

Our response

We will proceed with our proposal to apply rules and guidance as proposed in this policy statement to firms engaging in DeFi where a clear controlling person undertakes cryptoasset activities.

Applying our rules and guidance consistently where a clear controlling person exists will mitigate the risk of regulatory arbitrage between centralised and decentralised arrangements. We will assess whether a person is in scope of a regulated activity on a case-by-case basis.

We will also proceed with our work to consult on DeFi guidance late this year taking into account the feedback to CP25/40, CP26/13 and the DeFi workshops and industry engagement held between March and May 2026. The forthcoming guidance will seek to cover topics as proposed including indicators of (de)centralisation and guidance on how to mitigate operational resilience and financial crime risks when integrating or interacting with DeFi.

Chapter 10

Cost Benefit Analysis

10.1 Across multiple CPs we set out our cost benefit analysis (CBA) of the expected impact of our proposals for new cryptoasset activities which were entering into our regulatory perimeter as a result of Treasury legislation. These new activities included:

- Custody of Qualifying Cryptoassets (CP 25/14 and CP 25/25).
- Operating a Cryptoasset Trading Platform (CP 25/40).
- Cryptoasset Intermediation (CP 25/40).
- Cryptoasset Lending and Borrowing (CP 25/40 and CP 26/4).
- Cryptoasset Staking (CP 25/40 and CP 26/4).

10.2 In the CBA, our causal framework set out the expectation that introducing a regulatory regime for these activities would change firm behaviour and incentives to reduce harm to consumers in UK cryptoasset markets. At the same time, our assessment was that by introducing these activity specific rules, we would significantly reduce regulatory uncertainty for firms, which would increase market entry and support effective competition that benefits consumers.

10.3 Table 1 below summarises the key quantified and unquantified costs and benefits of our proposals to all market participants that were included within the CP25/14, CP25/25 and CP25/40 relating to our regulation of these cryptoasset activities. Total costs were estimated at £788m, with benefits estimated at £1.1bn. Costs were primarily driven by increased overheads to firms from compliance, while quantified benefits accrued to consumers as a result of increased regulatory protections.

10.4 Non-quantified costs include those associated with business model restrictions, that may require significant changes to how firms operate and generate revenue. We also noted a halo effect from regulation, which could result in consumers increasing investment into cryptoassets in the mistaken belief that regulation would prevent them from losses resulting from price volatility of cryptoasset products.

10.5 Qualitatively assessed benefits to firms included improved regulatory clarity, increased consumer demand for cryptoasset products (due to regulatory protections), and reduced risk aversion from the wider financial sector. We noted that these benefits are likely be significant, but we were unable to quantify them due to data limitations.

Table 1

Group Affected	Item Description	PV Benefits	PV Costs
Firms	Custody of Qualifying Cryptoassets	–	£290m
	Custody of Specified investment Cryptoassets	–	£12m
	Cryptoasset Trading Platforms	–	£79m
	Cryptoasset Intermediaries	–	£239m
	Cryptoasset Lending and Borrowing	–	£83m
	Cryptoasset Staking	–	£84m
Consumers	Reduced losses due to improved custody	£395m	–
	Value of regulatory protections	£745m	
Total impacts		£1,140m	£788m
Net impact		+£352m	
EANDCB		£66.4m	

Our response to feedback on the CBA

Across our multiple CPs concerning regulation of cryptoasset activities, we asked the following questions:

- **Question 1:** Do you agree with our assumptions and findings as set out in this CBA on the relative costs and benefits of the proposals contained in this consultation paper? Please give your reasons.
- **Question 2:** Do you have any views on the cost benefit analysis, including our analysis of costs and benefits to consumers, firms and the market?

In total we received 42 responses to question 1 and 37 responses to question 2 across our various CPs. Of these responses 35 came from firms, 5 came from trade groups, 3 from consumer groups and 4 from other market participants.

Rationale for Intervention

10.6 A small number of responses related to our description of why consumer harm materialises in cryptoasset markets, and why regulation is needed:

- One respondent challenged our suggestion that cryptoasset firms have misaligned incentives, rejecting the view that firms are insufficiently motivated to act in consumers' best interests. They also disagreed with the FCA's harm driver relating to information asymmetry and behavioural biases, disputing the claim that empirical evidence shows individuals are more willing to accept risk when investing in crypto.

Our response

We recognise that, as demonstrated through our regular survey data, a large share of consumers (47%) have positive experiences when engaging with UK cryptoasset markets and only a small portion (15%) say they regret their purchase. This suggests that for many cryptoasset consumers the market is functioning well. However, we have also seen repeated instances of consumer harm in UK cryptoasset markets, which in our assessment, materialise due to limited regulatory oversight and weak incentives to firms. When market crashes do occur, external research published by the Bank of International Settlement suggests retail consumers are more likely to experience losses due to behavioural heuristics such as herding and optimism bias (eg 'Buy the Dip'). As a result, we conclude these harms are present in UK cryptoasset markets and provide a rationale for our intervention.

Baseline, Counterfactual and Methodology

10.7 Some firms challenged the assumptions upon which we used to estimate our baseline for our analysis:

- Several firms questioned our assumption that 'the risk of regulatory arbitrage was low' or requested that additional analysis be undertaken to better model potential scenarios of consumers migrating to offshore platforms.
- Some respondents also queried our assessment of decentralised finance (DeFi) platforms, and how these would be impacted by our proposed rules, particularly in respect to enforcement challenges.

Our response

In relation to decentralised finance platforms, we have recently consulted on cryptoasset perimeter guidance (CP26/13) outlining how our rules apply to firms. This approach has informed our revised estimates of firms impacted by our rules, and which will as a result incur costs associated with our rules, and are accounted for within our CBA.

As set out in our CBA Statement of Policy, we generally assume there will be full compliance from firms with any new policy we implement.

Our modelling of benefits to consumers has likewise taken account of the platforms used by consumers to access cryptoasset markets. While we recognise consumers could seek to engage with unregulated platforms, based on our understanding of consumer behaviour, our assessment is that only a small share of total UK cryptoasset consumers would look to do so, and these consumers were already excluded from our assessment of benefits. As a result, we have not updated our analysis or assumptions in relation to consumer migration to unregulated platforms.

Estimates of costs

10.8 We received a wide range of feedback on our assessment of costs within our CBAs, with comments including:

- A number of firms queried our assessment of familiarisation costs, which were argued as too small for the familiarisation that would be required by firms, who will need external legal advice and substantial internal resources to interpret and operationalise the new rules.
- Some responses further suggested other operational costs appeared to be underestimated. An example given was IT system, which are expensive to operate and staff will be required for the relevant processes, which it was argued was not fully accounted for within the CBA.
- Many respondents also noted that our analysis indicated a concentration of compliance burdens on intermediaries.
- It was suggested that our analysis did not account for the costs of implementing an overall risk assessment (as required by authorisation) or certain ongoing costs associated with prudential requirements. These requirements create continuing operational obligations beyond initial authorisation and so should be accounted for within the CBA.
- One respondent, while agreeing with our overall assessment of costs, suggested that the most significant cost for many existing firms will be the technological and operational uplift required to move from unregulated operating models.
- It was also noted that consumers may face costs from our proposals, including temporary or permanent loss of access to certain tokens or services, friction as firms adjust onboarding and potential fee increases as firms absorb compliance costs.

Our response

Our estimates on familiarisation costs are informed using the FCA's standardised cost model, where we assumed firms would need to become familiar with consultation paper and legal text, and incur costs at a similar rate as current FSMA firms we authorise. Based on the feedback received, we have chosen to increase familiarisation costs to firms, recognising that the challenge of adapting business models from a non-regulatory to a regulated environment may require additional legal advice for firms. We have assumed firms will need to become familiar with a similar volume of text, but that they now incur costs at a higher rate, recognising a need for greater input from legal advisers.

We have not altered other cost estimates, on the basis that we did not receive sufficient feedback on how our cost estimates were inaccurate. Our costs represent mean averages, and as stated in our CBA, firms may in practice experience higher costs than those presented in our analysis.

In relation to distribution of costs, our analysis suggested intermediaries would share a higher portion of the total market cost, due to our expectation that the majority of firms would be authorised as intermediaries. On a per firm basis, we expect intermediaries to incur lower costs on average relative to trading platforms and custodians.

We recognise that there will be costs associated with cross-border cooperation. Given existing structures already in place, we have not attempted to identify the marginal impact of our rules on these costs but will look to monitor as our regime is implemented.

Costs relating to authorisation have been accounted for within the Treasury's assessment, and so we have not included them within our CBA to avoid double counting.

We recognise that firms may seek to pass costs on to consumers in the form of higher fees and prices. In practice, the extent to which firms are able to do so will depend on competitive dynamics, both within cryptoasset markets and between cryptoassets and substitute products. Our rules are intended to provide regulatory clarity to firms and increase market entry, which we expect in turn will increase effective competition in UK cryptoasset markets, which will benefit consumers.

In addition, our quantified estimates of costs to firms across our regime is smaller than our quantified estimate of benefits to consumers from our rules. As such, even if firms were able to fully pass on costs to consumers, we still anticipate our rules will result in net benefits to consumers, as a result of improved regulatory protections and reduced risk of harm. We will continue to closely monitor competitive outcomes in UK cryptoasset markets to ensure consumers receive good outcomes.

Benefits Estimation

10.9 We received a small number of comments that queried our estimate of the benefits of our proposed rules. Responses included:

- One firm challenged our 60% reduction in consumer losses from custody failures, stating that it seemed reasonable but optimistic.
- A firm also queried our estimate of consumer benefits materialising from improved regulatory protections (CP 25/40) noting that increased demand for cryptoassets would only partially benefit firms in the form of increased revenue from fees.
- Feedback also highlighted potential differences in the distribution of benefits, suggesting that there may be some groups of consumers who are likely to benefit from these rules more than others.
- One response agreed with our benefits estimation but suggested that capital inflows, innovation benefits, payments efficiency, and international competitiveness are underestimated.

Our response

We believe our assumption of custody failure reduction remains a best estimate of the likely impact of our proposed rules, although recognise high levels of uncertainty. This estimate is based on our assessment of the causes of custody failures and the recognition that custody failures do not always result in losses to consumers.

In addition, while we have made small amendments to our proposed custody rules following feedback from firms, we do not believe these materially change the risk to consumers. As a result, we have not changed our estimate of avoidable consumer losses due to our rules.

In addition, our survey data indicated an increase in average cryptoasset holdings by UK consumers, from £1,850 (in 2024) to £2,250 (in 2025). Furthermore, our behavioural experiment suggests consumers will on average increase their cryptoasset portfolio by 13% when receiving regulatory protections. As this will impact the avoided losses by consumers, we have updated our benefits estimation, accordingly, as outlined in Table 2 below.

In terms of regulatory protections benefiting market participants, we expect the majority of these benefits will be accrued by consumers, most of whom will welcome increased safeguards for their cryptoasset portfolios. However, increased demand from consumers will benefit firms in the form of higher fees and improved market liquidity. While we have not looked to separate these benefits between firms and consumers, our analysis suggests they will be significant, and we believe our estimate of these benefits remains valid.

We recognise that benefits may be unevenly distributed across consumers, and it is possible that consumers who are less active in cryptoasset markets, and who engage primarily via centralised exchanges will benefit more relative to consumers utilising self-storage solutions and engaging with DeFi applications. We have not attempted to disaggregate the distribution of benefits across consumers, although we will continue to monitor outcomes for consumers in cryptoassets markets, and take action to remedy unintended consequences as needed.

While we believe that capital inflow and efficiency benefits may be large, due to limited data availability and measurement challenges, we have not attempted to quantify these impacts. We remain of the view that the cumulative non-quantified benefits of our regime will be large and will exceed cumulative non-quantified costs.

Wider Economic Impacts

10.10 Many respondents provided feedback on our assessment of the wider economic impacts of our proposed rules:

- Multiple respondents mention they believe we have not fully considered the competition impacts of the rules. With a particular focus on the disproportionate impact, they believe the proposals will have on small firms, increasing barriers to entry or even leading to firm exit.
- Some respondents mentioned regulatory arbitrage as being a key factor in determining how much impact the proposals have on market participants. Both that there may be an increased incentive for some firms to not seek authorisation and to stay in jurisdictions with more preferential rules but also that consumer benefits will rely heavily on them not circumventing our rules.
- Respondents also mentioned that a need to consider the cumulative impact of the regime as a whole and not just this individual CP CBA.
- Firms also highlight potential adverse effects of our rules on innovation due to over-regulation. These responses suggested expanding the regulatory perimeter to non-custodial or open-source actors risks imposing high compliance costs without clear consumer benefit, potentially chilling innovation.
- One respondent stated that while alignment with international standards is important, it is important that the pursuit of competitiveness and growth should not weaken consumer protection or market integrity, which remain the FCA's primary objectives.

Our response

We have produced an overarching CBA that combines all relevant cryptoasset CBAs (CP 25/14, CP 25/15, CP 25/25, CP 25/40, CP 25/41, CP 25/42 and CP 26/4) into a single analysis, which is being published alongside this document. This CBA considers the regime at a whole and the cumulative impact of the rules.

In relation to our assessment of the impact of our rules on competition, we have looked to account for this feedback within the aggregate cryptoasset CBA. Our assessment is limited by data constraints which prevents us from more accurately determining the competitive dynamics especially around firm entry and exit. However, we recognise that our rules will affect competition in this market and will continue to monitor outcomes to ensure this market delivers effective competition which benefits consumers, in line with our primary objectives.

We acknowledged a risk of regulatory arbitrage within our CBA but stated that as our rules are built on global cryptoasset regulatory standards set by IOSCO, FSB and FATF, this risk would be low. In addition, we assumed that widespread consumer leakage to unregulated overseas platforms is unlikely to be significant, given the scope of our rules and our consumer survey data indicating the vast majority of consumers rely

on centralised platforms. While there may be some consumers seeking to access offshore and unregulated platforms to access cryptoassets not available in UK markets, we believe this is likely to be a very small subgroup of consumers. Based on this assessment, we anticipate the risks of regulatory arbitrage and consumer leakage remain low, and so are unlikely to materially impact our estimates of the overall benefits of our proposed regime.

We recognise that innovation is a core driver of economic growth, and our rules are designed in a way to encourage firms to innovate while reducing risks from consumers. While in certain cases regulation can deter innovation, a lack of regulatory clarity can prevent firms from entering into markets and creating new and innovative products. We have observed strong interest in our digital regulatory sandboxes since launch, and believe our rules strike the right balance between encouraging innovation and protecting consumers.

In terms of distribution of benefits, our CBA represented our best estimate of how and where these would materialise, given our limited data sources. We do not consider it reasonably proportionate or feasible to collect higher quality and more granular data on the distribution of benefits for this CBA, and so we have not updated our analysis. As noted in the CBA, we will continue to monitor outcomes for consumers and market participants in UK participants as our rules are implemented, which we expect will allow us to better assess the distribution of benefits from our cryptoasset regime.

Monitoring and Evaluation

10.11 Some of the feedback we received related to our proposed approach to monitoring outcomes of the regime:

- One response suggested a need for ongoing monitoring to ensure costs are not unfairly passed on to retail consumers, consumer protection remains effective as the market develops, and smaller, innovative firms are not crowded out.
- This response also highlighted a risk that sharp market downturns could harm vulnerable consumers and spill over into the wider financial system, with these economy-wide risks needing ongoing oversight.
- Another respondent suggested using metrics like complaints volumes, disruptions, execution quality and failed withdrawals to measure the success of our regime.

Our response

We agree that monitoring outcomes of our regime will be critical to ensure its success and avoiding unintended consequences. As set out in our CBA, we intend to actively monitor UK cryptoasset markets to ensure our rules produce the benefits intended. We will also look to conduct and publish an evaluation of our cryptoasset regime at a future date.

Updated Cost Estimates

10.12 In Table 2 below, we provide an update of cost estimates based on the changes made between our CP and Policy Statement, namely:

- An increased firm population.
- Higher per firm familiarisation costs.
- Increased benefits from our custody rules (due to updated survey data suggesting higher average UK holdings).

Table 2

Regulatory Requirement	Transition Costs (per firm)	Transition Costs (population)	Ongoing Costs (per firm)	Ongoing Costs (population)	Total population cost (PV across 10 year appraisal period)
Cryptoasset Custody	£1.8m	£110m	£0.6m	£37m	**£315m**
Cryptoasset Trading Platforms	£1.9m	£8.5m	£2.0m	£9.1m	**£84m**
Cryptoasset Intermediaries	£0.2m	£37.5m	£0.2m	£50.6m	**£355m**
Lending and Borrowing	£0.4m	£5.6m	£0.7m	£8.6m	**£85m**
Staking	£0.3m	£15.8m	£0.2m	£10.3m	**£85m**
Total Costs					**£920m**

10.13 As seen above, total costs have increased, largely driven by an increased number of market participants which we expect to be within scope of the regime. We expect the non-quantified benefits to be significant and to exceed the costs to firms.

Annex 1

List of non-confidential respondents

AFME

Animoca Brands

Association of Corporate Treasurers

Avian labs

Blockchain and Climate Institute

British Blockchain Association

British Standards Institution

Capital Law

CertiK

Cleartoken Depository Ltd

Coinbase

Crypto UK

Digital Token Identifier Foundation

Dumpling

Emmanuel Young

Everstake

Figment

Financial Services Consumer Panel

gunnercooke llp

Herodotus Dev Ltd

ICAEW

International Securities Lending Association

Kiln

Kris Tokarzewski

Ledger

Lloyds

Lysis Group

NatWest

Portofino Technologies UK Ltd

UK Centre for Blockchain Technologies

UK Crypto Business Council (UKCBC)

UK Finance

University of East London – Centre of Fintech

Upbit

Yousaf Ahmed

Annex 2

Abbreviations used in this paper

Abbreviation	Description
A&D	Admissions and Disclosures
AIF	FCA's Approach to International Firms
AICF	Approach to International Cryptoasset Firms
AIFM	Alternative Investment Fund Manager
CASS	Client Assets Sourcebook
CARF	Cryptoasset Reporting Framework
CATP	Cryptoasset Trading Platform
CBA	Cost Benefit Analysis
CfD	Contracts for Difference
COBS	Conduct of Business Sourcebook
CP	Consultation Paper
CRYPTO	The Crypto Sourcebook
CSD	Central Securities Depository
DeFi	Decentralised Finance
DISP	Dispute Resolution: Complaints Sourcebook
DLT	Distributed Ledger Technology
DP	Discussion Paper
DTI	Digital Token Identifier
EANDCB	Equivalent Annual Net Direct Cost to Business
EU	European Union

Abbreviation	Description
FCA	Financial Conduct Authority
FSMA	Financial Services and Markets Act 2000
HMRC	HM Revenue and Customs
HSM	Hardware Security Modules
IOSCO	International Organization of Securities Commissions
L&B	Cryptoasset lending and cryptoasset borrowing
LTV	Loan-To-Value
MARC	Market Abuse Regime for Cryptoassets
MiFID	Markets in Financial Instruments Directive
MiFIR	Markets in Financial Instruments Regulation
MLRs	Money Laundering Regulations
MPC	Multi-Party Computation
MPT	Matched Principal Trading
MTF	Multilateral Trading Facility
PFOF	Payment For Order Flow
PRz	Prescribed Responsibility
PERG	The Perimeter Guidance Manual
PRIN	Principles for Businesses
PS	Policy Statement
PV	Present Value
QCATP	Qualifying Cryptoasset Trading Platform
QCDD	Qualifying Cryptoasset Disclosure Document(s)
RAO	Regulated Activities Order 2001
RSIC	Relevant Specified Investment Cryptoasset

Abbreviation	Description
RTS	Regulatory Technical Standard
SDD	Supplementary Disclosure Document
SI	Systematic Internaliser
SIC	Specified Investment Cryptoasset
SM&CR	Senior Managers & Certification Regime
SUP	Supervision Sourcebook
SYSC	Senior Management Arrangements, Systems and Controls
T&Cs	Terms and Conditions
TradFi	Traditional Finance
TTCA	Title Transfer Collateral Arrangement
UK QCATP	UK-authorised Qualifying Cryptoasset Trading Platform
UK MAR or MAR	UK Market Abuse Regulation
USDC	US dollar-denominated stablecoin
UTC	Coordinated Universal Time

Appendix 1

Made rules (legal instrument)

GLOSSARY (CRYPTOASSETS) 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"), including as applied by article 98 (Application of section 137B of the Act to backing assets for qualifying stablecoin) of the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (SI 2001/544) (as amended by the Financial Services and Markets Act 2000 (Cryptoassets) Regulations 2026 (SI 2026/102)) as applied by paragraph 3 (FCA rules) of Part 1 (Application and modification of the 2000 Act) of Schedule 6 (Application and modification of legislation) to the Payment Services Regulations 2017 (SI 2017/752) and paragraph 2A (Authority rules) of Part 1 (Application and modification of legislation) of Schedule 3 (Application and modification of legislation) to the Electronic Money Regulations 2011 (SI 2011/99):

(a) section 71N (Designated activities: rules);
(b) section 137A (The FCA's general rules);
(c) section 137B (FCA general rules: clients' money, right to rescind etc.);
(d) section 137R (Financial promotion rules); and
(e) section 137T (General supplementary powers);
(f) section 213 (The compensation scheme);
(g) section 214 (General);
(h) section 226 (Compulsory jurisdiction); and
(i) paragraph 13 (FCA's rules) of Part III (The Compulsory Jurisdiction) of Schedule 17 (The Ombudsman Scheme);

(2) the following provisions of the Financial Services and Markets Act 2000 (Cryptoassets) Regulations 2026 (SI 2026/102):

(a) regulation 6 ("Qualifying cryptoasset disclosure document" and "supplementary disclosure document");
(b) regulation 9 (Designated activity rules: qualifying cryptoasset public offers and admissions to trading);
(c) regulation 12 (Responsibility for disclosure documents);
(d) regulation 13 (General requirements to be met by a qualifying cryptoasset disclosure document or supplementary disclosure document);
(e) regulation 15 (Withdrawal rights);
(f) regulation 21 (Designated activity rules: market abuse in qualifying cryptoassets and related instruments);
(g) regulation 23 (Exclusions: insider dealing);
(h) regulation 26 (Public disclosure of inside information);
(i) regulation 27 (Public disclosure of inside information: delayed disclosure);

(j) regulation 30 (Systems and procedures for trading relevant qualifying cryptoassets and related instruments);
(k) regulation 31 (Insider lists for relevant qualifying cryptoassets and related instruments);
(l) regulation 32 (Cases in which sharing of information authorised or required);
(m) regulation 34 (Legitimate cryptoasset market practice);
(n) regulation 36 (Disapplication or modification of rules); and
(o) paragraph 8 ("Protected forward-looking statement") of Part 2 (Further exemption relating to forward-looking statement) of Schedule 2 (Compensation: exemptions); and

(3) the other rule 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 Consequentials) Instrument 2026;
(10) Cryptoassets (Conduct and Firm Standards) Instrument 2026; and
(11) Cryptoassets (COREPRU and CRYPTOPRU) Instrument 2026.

Amendments to the Handbook

D. The Glossary of definitions is amended in accordance with the Annex to this instrument.

Notes

E. In the Annex to this instrument, the notes (indicated by "*Editor's note*:") are included for the convenience of readers but do not form part of the legislative text.

Citation

F. This instrument may be cited as the Glossary (Cryptoassets) Instrument 2026.

By order of the Board
25 June 2026

Annex

Amendments to the Glossary of definitions

In this Annex, underlining indicates new text and striking through indicates deleted text, unless stated otherwise.

Insert the following new definitions in the appropriate alphabetical position. The text is not underlined.

admission criteria	(in *CRYPTO* 3) the criteria a *retail UK QCATP operator* is required to establish by *CRYPTO* 3.2.5R.
arranging (bringing about) deals in qualifying cryptoassets	the *regulated activity* specified in article 9Y(1) of the *Regulated Activities Order* (Arranging deals in qualifying cryptoassets), which is, in summary, making arrangements for another *person* (whether as *principal* or agent) to *buy*, *sell*, subscribe for or underwrite a *qualifying cryptoasset*.
arranging cryptoasset safeguarding	the *regulated activity* specified in article 9N(1)(b) of the *Regulated Activities Order* (Safeguarding of qualifying cryptoassets and relevant specified investment cryptoassets).
arranging deals in qualifying cryptoassets	the *regulated activity* specified in article 9Y of the *Regulated Activities Order* (Arranging deals in qualifying cryptoassets), which is, in summary, making arrangements for either or both of the following: (a) for another *person* (whether as *principal* or agent) to *buy*, *sell*, subscribe for or underwrite a *qualifying cryptoasset*; and (b) with a view to a *person* who participates in the arrangements for the *buying*, *selling*, subscribing for or underwriting of a *qualifying cryptoasset*, whether as *principal* or agent.
arranging qualifying cryptoasset safeguarding	the *regulated activity* specified in article 9N(1)(b) (Safeguarding of qualifying cryptoassets and relevant specified investment cryptoassets) of the *Regulated Activities Order*, but only in relation to *qualifying cryptoassets*.
arranging qualifying cryptoasset staking	the *regulated activity* specified in article 9Z6 (Qualifying cryptoasset staking) of the *Regulated Activities Order*, which is, in summary, making arrangements on behalf of another (whether as *principal* or agent) for *qualifying cryptoasset staking*.

authorised cryptoasset firm	an *authorised person* who has a *Part 4A permission* to carry on a *regulated cryptoasset activity*.
backing asset composition requirement	the requirement in *CASS* 16.2.25R.
backing asset pool	(a) a pool of *money* and/or *assets* held by a *firm* in connection with a *qualifying stablecoin* with a view to maintaining the stability or value of that *qualifying stablecoin*; and (b) any additional sum held in excess of the requirement in *CASS* 16.2.1R(3) in accordance with *CASS* 16.4.16R.
backing asset pool acknowledgement letter	a letter in the form set out in *CASS* 16 Annex 1.
backing assets account	an account in which a *qualifying stablecoin issuer* holds *assets* in the *backing asset pool*.
backing funds account	an account in which a *qualifying stablecoin issuer* holds *money* in the *backing asset pool*.
blockchain validation	(in accordance with article 9Z6 (Qualifying cryptoasset staking) of the *Regulated Activities Order*) the validation of transactions on: (a) a blockchain; or (b) a network that uses distributed ledger technology or other similar technology, and includes proof of stake consensus mechanisms.
burning	the process by which a *cryptoasset* is permanently removed from circulation on a blockchain or other network that uses distributed ledger technology or other similar technology.
client cryptoasset	a *qualifying cryptoasset* which is either: (a) required to be held in trust under *CASS* 17.3.3R by a *firm* to which that *rule* applies; or (b) part of an *operational surplus*.
client cryptoasset discrepancy record	a *firm's* record setting out details of each discrepancy relating to its safeguarding of *client cryptoassets* that it identifies under *CASS* 17.5.11R, as required under *CASS* 17.5.11R(2).

client cryptoasset reconciliation	the process set out at *CASS* 17.5.10R.
client cryptoasset reconciliation record	a *firm's* record setting out details of each *client cryptoasset reconciliation* which it performs under *CASS* 17.5.10R, as required under *CASS* 17.5.10R(4).
client cryptoasset third party due diligence record	a *firm's* record of the grounds upon which an appointment of a third party under *CASS* 17.6.3R or *CASS* 17.6.8R met the requirements of *CASS* 17.6.3R(1) or *CASS* 17.6.8R(2), as required by *CASS* 17.6.11R(1).
client cryptoasset third party governance record	a *firm's* record of its *governing body's*, or its *governing body's* delegate's, approval under *CASS* 17.6.9R(1) or (3), as required under *CASS* 17.6.11R(5).
client cryptoasset third party review record	a *firm's* record of the conclusions of any periodic review performed under *CASS* 17.6.5R or *CASS* 17.6.8R(4), as required under *CASS* 17.6.11R(3).
client cryptoasset trust exemption consent record	a record of a *firm's client's* written consent under *CASS* 17.3.5R(4) or *CASS* 17.3.6R(1)(c) for the *firm* to use the exemption at *CASS* 17.3.5R(1) or *CASS* 17.3.6R(1) respectively, as required under *CASS* 17.3.11R(4).
client cryptoasset trust exemption record	a record of a *firm's* reasons for concluding that it is necessary for the exemption at *CASS* 17.3.6R(1) to be used, as required under *CASS* 17.3.6R(3).
client cryptoasset trust record	a *firm's* record of a trust that it has created under *CASS* 17.3.3R, as required under *CASS* 17.3.19R.
core backing asset requirement	the requirement in *CASS* 16.2.27R.
core backing assets	(a) *on-demand deposits*; and (b) *short-term government debt instruments*.
CRYPTO	the Cryptoassets sourcebook.
cryptoasset	as defined in section 417 (Definitions) of the *Act*, any cryptographically secured digital representation of value or contractual rights that: (a) can be transferred, stored or traded electronically; and (b) uses technology supporting the recording or storage of data (which may include distributed ledger technology).

cryptoasset inside information	'inside information' as defined in regulation 18 (Inside information) of the *Cryptoassets Regulations*.
cryptoasset insider	a *person* who possesses inside information, as described in regulation 22(4) and (5) (Prohibited use of inside information (insider dealing)) of the *Cryptoassets Regulations*.
cryptoasset insider dealing	using inside information as prohibited by regulation 22 (Prohibited use of inside information (insider dealing)) of the *Cryptoassets Regulations*.
cryptoasset insider list	a list, as required by regulation 31(1)(a) (Insider lists for relevant qualifying cryptoassets and related instruments) of the *Cryptoassets Regulations*, of all *persons* specified in *CRYPTO* 4.12.2R, who: (a) have access to *cryptoasset inside information*; and (b) are working for those *persons* under a contract of employment, or otherwise performing tasks through which they have access to *cryptoasset inside information*, such as advisers, accountants or credit rating agencies.
cryptoasset intermediary	an *authorised person*, other than a *UK QCATP operator*, that carries out any of the following activities: (a) in relation to *qualifying cryptoassets*: (i) *dealing in qualifying cryptoassets as principal*; (ii) *dealing in qualifying cryptoassets as agent*; and (iii) *arranging deals in qualifying cryptoassets*; and (b) in relation to *related instruments*: (i) *dealing in investments as principal*; (ii) *dealing in investments as agent*; (iii) *arranging (bringing about) deals in investments*; and (iv) *making arrangements with a view to transactions in investments*.
cryptoasset market abuse	any activity prohibited by the following provisions in the *Cryptoassets Regulations*:

	(a) regulation 22 (Prohibited use of inside information (insider dealing));
	(b) regulation 24 (Prohibition on the disclosure of inside information); and
	(c) regulation 28 (Prohibition of market manipulation).
cryptoasset market manipulation	'market manipulation' as defined in regulation 19 (Market manipulation) of the *Cryptoassets Regulations*.
cryptoasset means of access record	a *firm's* record setting out details of each *means of access* it controls at any particular point in time, as required under *CASS* 17.4.8R.
cryptoasset safeguarding arrangement record	a *firm's* record of *arranging qualifying cryptoasset safeguarding*, as required under *CASS* 17.7.3R(1).
cryptoasset safeguarding class	a class of *cryptoasset* in which all the *cryptoassets*:
	(a) are fungible with each other;
	(b) are instances of the same single product;
	(c) share the same name or identifier code; and
	(d) exist on:
	(i) the same blockchain; or
	(ii) the same network that uses distributed ledger technology or other similar technology.
cryptoasset safeguarding rules	*CASS* 17.
cryptoasset unlawful disclosure	the behaviour described in regulation 24 (Prohibition on the disclosure of inside information) of the *Cryptoassets Regulations*.
Cryptoassets Regulations	The Financial Services and Markets Act 2000 (Cryptoassets) Regulations 2026 (SI 2026/102).
dealing in qualifying cryptoassets (as principal or agent)	one or both of the following activities:
	(a) *dealing in qualifying cryptoassets as principal*; and
	(b) *dealing in qualifying cryptoassets as agent*.

dealing in qualifying cryptoassets as agent	the *regulated activity*, specified in article 9W (Dealing in qualifying cryptoassets as agent) of the *Regulated Activities Order*, which is, in summary, *buying*, *selling*, subscribing for or underwriting *qualifying cryptoassets* as agent.
dealing in qualifying cryptoassets as principal	the *regulated activity*, specified in article 9T (Dealing in qualifying cryptoassets as principle) of the *Regulated Activities Order*, which is, in summary, *buying*, *selling*, subscribing for or underwriting *qualifying cryptoassets* as principal.
digital token identifier	an identifier: (a) which is a digital token identifier available on the Digital Token Identifier Foundation Registry; or (b) if there is no digital token identifier available for the purposes of (a), which clearly describes the *qualifying cryptoasset* and is each of the following: (i) unique; (ii) neutral; (iii) reliable; (iv) open source; (v) accessible; and (vi) subject to a governance framework.
expanded backing assets	in relation to a *backing asset pool*, the following *assets*: (a) *long-term government debt instruments*; (b) units in a *fund* which is authorised as a *public debt CNAV MMF* under the *Money Market Funds Regulation* or the *EU MMF Regulation* and which meets the following conditions: (i) all *asset*s held within the *fund* are denominated in the *reference currency* of the *qualifying stablecoin*; and (ii) *asset*s which are a debt security represent a claim on the *UK* government or the central government of a *Zone A country*; and

(c) *asset*s, rights or *money* held as a counterparty to a *repurchase transaction* (whether as a repurchase agreement or reverse repurchase agreement):

(i) that has a maximum maturity up to and including 7 *days*;

(ii) that concerns *long-term government debt instruments* or *short-term government debt instruments*; and

(iii) in relation to which the other counterparty is limited to one of the following:

(A) a *UK credit institution*;

(B) a *MIFIDPRU investment firm*;

(C) a *designated investment firm*;

(D) a 'UK Solvency II firm' as defined in chapter 2 of the PRA Rulebook: Solvency II Firms Insurance General Application; or

(E) a *third country person* with a main business comparable to any of the entities referred to in (A) to (D).

EU MMF Regulation the *EU* version of Regulation (EU) No. 2017/1131 of the European Parliament and the Council of 14 June 2017 on money market funds.

FCA-owned centralised repository (in *CRYPTO*) the system identified by the *FCA* on its website as the centralised repository for information relating to *qualifying cryptoassets*.

issuing a qualifying stablecoin the activity defined in article 9M (Issuing qualifying stablecoin) of the *Regulated Activities Order*.

large CATP operator a *firm* which:

(a) operates a *UK QCATP*;

(b) has average revenue, to be calculated at 12-*month* intervals, of more than or equal to £10m a year, for the 3 previous years, having regard to:

(i) all its activities, including but not limited to operating a *UK QCATP*; and

	(ii) where applicable, revenue arising from periods when the business was carried on by or in any predecessor entity.
legal entity identifier	(in *CRYPTO*) a 20-character alphanumeric code that uniquely identifies legally distinct entities which engage in financial transactions.
legitimate cryptoasset market practice	a market practice that is specified in *CRYPTO* 4.11.
LEI	a *legal entity identifier*.
long-term government debt instrument	a debt security representing a claim on the *UK* government or the central government of a *Zone A country* with a residual maturity of more than 365 *days*.
making arrangements with a view to transactions in qualifying cryptoassets	the *regulated activity* specified in article 9Y(2) of the *Regulated Activities Order* (Arranging deals in qualifying cryptoassets), which is, in summary, making arrangements with a view to a *person* who participates in the arrangements for the *buying*, *selling*, subscribing for, or underwriting of a *qualifying cryptoasset*, whether as *principal* or agent.
means of access	a private cryptographic key, part or parts of a private cryptographic key or some other means of which, in either case, a *person* would need possession or knowledge to bring about a transfer of the benefit of a *cryptoasset* to another *person*.
minting	the process of putting a *cryptoasset* on a blockchain or other network using distributed ledger technology or similar technology in a transferrable form.
offer of a qualifying cryptoasset to the public	has the same meaning as in regulation 5 ("Offer of a qualifying cryptoasset to the public") of the *Cryptoassets Regulations*.
on-demand deposit	a *deposit* the terms of which require that the sum of *money* paid will be repaid, with or without interest or a premium, on demand.
on-demand deposit requirement	the requirement in *CASS* 16.2.1R(4).
operational surplus	one or more *qualifying cryptoassets* or *relevant specified investment cryptoassets* which a *firm* is using in accordance with *CASS* 17.3.20R.

operating a qualifying CATP	the *regulated activity* in article 9S (Operating a qualifying cryptoasset trading platform) of the *Regulated Activities Order* which is, in summary, the operation of a *qualifying cryptoasset trading platform*.
person responsible for the offer	(in accordance with regulation 3(3) (Interpretation: qualifying cryptoasset public offers and admissions to trading) and regulation 17(1) and (5) (Interpretation: market abuse in qualifying cryptoassets and related instruments) of the *Cryptoassets Regulations*): (a) in relation to the *offer of a qualifying cryptoasset* to the public: (i) the *person* making the offer; or (ii) where the offer is being made on behalf of another, the *person* on whose behalf the offer is being made; (b) in relation to the *admission to trading* of a *qualifying cryptoasset* on a *UK QCATP*: (i) the *person* requesting or obtaining *admission to trading*; or (ii) where, of its own motion, a *UK QCATP operator* admits a *qualifying cryptoasset* to trading on a *UK QCATP* operated by it, that *UK QCATP operator*; or (c) in relation to a *related instrument*, the *person* who is, for the purposes of the *Market Abuse Regulation*, the offeror of that instrument.
per-trust operational surplus record	a *firm's* record, in relation to a trust created by it under *CASS* 17.3.3R, of the reasons for it being necessary for the *firm* to use an *operational surplus* for that trust, as required under *CASS* 17.3.20R(4).
per-trust/class cryptoasset resource	the amount of a particular class of *client cryptoasset* that a *firm* is required to confirm under *CASS* 17.5.7R that it is safeguarding for *clients* under a particular trust in accordance with *CASS* 17.3.3R.
per-trust/client/class cryptoasset requirement	the amount of a particular class of *client cryptoasset* that a *firm* is required to hold for a particular *client* under a particular trust in accordance with *CASS* 17.3.3R, as calculated at *CASS* 17.5.6R.

pre-issued stablecoin	a *qualifying stablecoin* that first entered circulation prior to 25 October 2027.
proprietary token	a *qualifying cryptoasset* that is not a *UK qualifying stablecoin* and that is either: (a) a *qualifying cryptoasset* issued by a *qualifying cryptoasset firm* or a member of its *group*; or (b) a *qualifying cryptoasset* over which a *qualifying cryptoasset firm* or a member of its *group* has material control or holdings of its supply.
public debt CNAV MMF	(a) in relation to a *regulated money market fund*, has the meaning given in article 2(11) (Definitions) of the *Money Market Funds Regulation*; or (b) in relation to a money market fund authorised under the *EU MMF Regulation*, has the meaning given in article 2(11) (Definitions) of the *EU MMF Regulation*.
QCATP	a *qualifying cryptoasset trading platform*.
QCATP operator	a *qualifying CATP operator*.
QCDD	a document which is a qualifying cryptoasset disclosure document for the purposes of Chapter 1 (Qualifying cryptoasset public offers and admissions to trading) of Part 2 (Markets in cryptoassets: designated activities) of the *Cryptoassets Regulations*.
qualifying CATP	a *qualifying cryptoasset trading platform*.
qualifying CATP operator	a *firm* authorised to carry on the activity of *operating a qualifying CATP*.
qualifying cryptoasset activity	any of the following activities, specified in Part II of the *Regulated Activities Order* (Specified Activities): (a) *issuing a qualifying stablecoin* (article 9M (Issuing qualifying stablecoin)); (b) *safeguarding cryptoassets* (article 9N(1)(a) (Safeguarding of qualifying cryptoassets and relevant specified investment cryptoassets)); (c) *arranging cryptoasset safeguarding* (article 9N(1)(b)); (d) *operating a qualifying CATP* (article 9S (Operating a qualifying cryptoasset trading platform));

	(e) *dealing in qualifying cryptoassets as principal* ((article 9T (Dealing in qualifying cryptoasset trading platform) (but disregarding the exclusion in article 9U (Article 9T exclusion: absence of holding out etc.));
	(f) *dealing in qualifying cryptoassets as agent* (article 9W (Dealing in qualifying cryptoassets as agent));
	(g) *arranging deals in qualifying cryptoassets* (article 9Y (Arranging deals in qualifying cryptoassets)); or
	(h) *arranging qualifying cryptoasset staking* (article 9Z6 (Qualifying cryptoasset staking)).
qualifying cryptoasset best execution obligation	(in *CRYPTO* 5) the obligation of a *firm* under *CRYPTO* 5.4.1R, *CRYPTO* 5.4.10R, *CRYPTO* 5.4.13R and *CRYPTO* 5.4.16R.
qualifying cryptoasset borrowing	the disposal of a *qualifying cryptoasset* from or via an *authorised cryptoasset firm* to a *person* subject to an obligation or right to reacquire the same or equivalent *qualifying cryptoasset* from the *person*, which may include the provision of *qualifying cryptoasset borrowing collateral* and/or payment of interest from the *person* to the *authorised cryptoasset firm*.
qualifying cryptoasset borrowing collateral	the transfer (other than by way of sale) by a *retail client* of assets (including *qualifying cryptoassets*) or currency, or rights in respect thereof, subject to a right of the *retail client* to have transferred back to them the same or equivalent assets or currency where the assets or currency are transferred to secure the performance of the obligations of the *retail client* arising in connection with *qualifying cryptoasset borrowing*.
qualifying cryptoasset custodian	an *authorised person* with *permission* to carry on the *regulated activity* of *safeguarding cryptoassets*.
qualifying cryptoasset execution venue	(in *CRYPTO*):
	(a) a *qualifying cryptoasset trading platform*;
	(b) a single dealer platform;
	(c) a liquidity provider; or
	(d) an entity that, in a *third country*, performs a similar function to the functions performed by any of the entities in (a) to (c).

qualifying cryptoasset firm	a *firm* with a *Part 4A permission* which includes a *qualifying cryptoasset activity*.
qualifying cryptoasset lending	the disposal of a *qualifying cryptoasset* from a *person* to or via an *authorised cryptoasset firm* subject to an obligation or right to reacquire the same or equivalent *qualifying cryptoasset* from the *authorised cryptoasset firm*, typically with compensation paid to that *person* by the *qualifying cryptoasset firm* in the form of yield.
qualifying cryptoasset lending or borrowing	one or both of the following services: (a) *qualifying cryptoasset lending*; and (b) *qualifying cryptoasset borrowing*.
qualifying cryptoasset staking	the use of a *qualifying cryptoasset* in *blockchain validation*.
qualifying cryptoasset trading platform	(in accordance with article 3(1) (Interpretation) of the *Regulated Activities Order*) a system which brings together, or facilitates the bringing together of, multiple third-party *buying* and *selling* interests in *qualifying cryptoassets* in a way that results in a contract for the exchange of *qualifying cryptoassets* for: (a) *money* (including *electronic money*); or (b) other *qualifying cryptoassets*.
qualifying stablecoin	the specified *investment* defined in article 88G (Qualifying stablecoin) of the *Regulated Activities Order*.
qualifying stablecoin funds	(a) *money* received by a *qualifying stablecoin issuer* in payment for a *qualifying stablecoin* in the course of carrying out the activity of *issuing a qualifying stablecoin*; and (b) *money* that is equivalent in value to the consideration accepted by a *qualifying stablecoin issuer* when it accepts something other than *money* in payment for a *qualifying stablecoin* in the course of carrying out the activity of *issuing a qualifying stablecoin*.
qualifying stablecoin issuer	an *authorised person* with *permission* to carry on the *regulated activity* defined in article 9M (Issuing qualifying stablecoin) of the *Regulated Activities Order*.
qualifying stablecoin product	a category of *qualifying stablecoins* identifiable on the basis that:

(a) each *qualifying stablecoin* within that category is fungible with each other *qualifying stablecoin* within that category; and

(b) together all the *qualifying stablecoins* in that category represent a single product.

qualifying stablecoin product identifier

the following identifiers in respect of a *qualifying stablecoin product* and the *qualifying stablecoins* within it:

(a) the name of the *qualifying stablecoin product* and, if different, that part of the name used by all *qualifying stablecoins* in the *qualifying stablecoin product*; and

(b) any *digital token identifiers* relating to the *qualifying stablecoin product* (including those for equivalent groups on the Digital Token Identifier Foundation Registry).

redemption day

(a) a *business day*; or

(b) any other *day* on which a *qualifying stablecoin issuer* is operating so as to be able to complete *redemptions*.

redemption fee

the fee a *qualifying stablecoin issuer* charges for carrying out *redemption*.

redemption sum

the *reference value* of the sum total of *qualifying stablecoins* in respect of which a *redemption* request is received, less:

(a) any *redemption fee*; and

(b) any currency exchange fees which may be incurred by the *qualifying stablecoin issuer* in meeting the *redemption* request in a currency chosen by the *holder* where that currency is different to the *reference currency*.

reference currency

the fiat currency to which a *qualifying stablecoin* is referenced.

reference value

the face value of a *qualifying stablecoin*, with reference to a unit of the fiat currency to which that *qualifying stablecoin* is referenced.

regulated cryptoasset activity

the *regulated activities* in Chapter 2B (Cryptoassets) of Part II (Specified activities) of the *Regulated Activities Order*:

(a) *issuing a qualifying stablecoin*;

(b) *safeguarding cryptoassets*;

(c) *arranging cryptoasset safeguarding*;

(d) *operating a qualifying CATP*;

(e) *dealing in qualifying cryptoassets as principal*;

(f) *dealing in qualifying cryptoassets as agent*;

(g) *arranging (bringing about) deals in qualifying cryptoassets*;

(h) *making arrangements with a view to transactions in qualifying cryptoassets*; and

(i) *arranging qualifying cryptoasset staking*.

related instrument (in accordance with regulation 17(1) (Interpretation: market abuse in qualifying cryptoassets and related instruments) of the *Cryptoassets Regulations*) a *financial instrument* or *specified investment* whose price or value depends on, or has an effect on, the price or value of a *relevant qualifying cryptoasset*, but does not include a *financial instrument* or *specified investment* which:

(a) is a *relevant qualifying cryptoasset*; or

(b) falls within article 2(1) (Scope) of the *Market Abuse Regulation*.

relevant dealer in principal (in accordance with regulation 17(1) (Interpretation: market abuse in qualifying cryptoassets and related instruments) of the *Cryptoassets Regulations*) a *person* who carries on an activity of a kind described in article 9T (Dealing in qualifying cryptoassets as principal) of the *Regulated Activities Order* in relation to a *relevant qualifying cryptoasset*.

relevant issuer (in accordance with regulation 17(1) (Interpretation: market abuse in qualifying cryptoassets and related instruments) of the *Cryptoassets Regulations*):

(a) in relation to a *relevant qualifying cryptoasset*:

(i) the issuer of a *qualifying stablecoin*; or

(ii) in any other case, a *person* ('A') where:

(A) A offers a *qualifying cryptoasset*, or arranges for another to offer that *qualifying cryptoasset* to the public; and

	(B) that *qualifying cryptoasset* is created by, or on behalf of, A for sale or subscription; or
	(b) in relation to a *related instrument*, the issuer of that instrument.
relevant qualifying cryptoasset	(in accordance with regulation 17(1) (Interpretation: market abuse in qualifying cryptoassets and related instruments) of the *Cryptoassets Regulations*) a *qualifying cryptoasset* that has been *admitted to trading*, or is subject to an application seeking *admission to trading*, on a *UK QCATP*.
relevant specified investment cryptoasset	a *specified investment cryptoasset* which meets the definition at article 9N(5)(b) (Safeguarding of qualifying cryptoassets and relevant specified investment cryptoassets) of the *Regulated Activities Order*.
reportable post-trade transparency information	information which a *transparency reporting firm* is required to report, as set out in *CRYPTO* 7.3.
reportable pre-trade transparency information	information which a *transparency reporting firm* is required to report, as set out in *CRYPTO* 7.2.
retail UK QCATP	a *UK QCATP* whose rules do not preclude *retail investors* from trading on the *UK QCATP* directly or through intermediaries.
retail UK QCATP operator	the operator of a *retail UK QCATP*.
safeguarding cryptoassets	the *regulated activity* specified in article 9N(1)(a) (Safeguarding of qualifying cryptoassets and relevant specified investment cryptoassets) of the *Regulated Activities Order*.
safeguarding qualifying cryptoassets	the *regulated activity* specified in article 9N(1)(a) (Safeguarding of qualifying cryptoassets and relevant specified investment cryptoassets) of the *Regulated Activities Order*, but only in relation to *qualifying cryptoassets*.
safeguarding qualifying cryptoassets and relevant specified investment cryptoassets	*safeguarding cryptoassets*.
short-term government debt instrument	a debt security representing a claim on the *UK* government or the central government of a *Zone A country* with a residual maturity of 365 *days* or fewer.

specified investment cryptoasset	a *cryptoasset* that: (a) is a *specified investment* as a result of Part III (Specified investments) of the *Regulated Activities Order*: (i) excluding article 88F (Qualifying cryptoassets); and (ii) including where the *cryptoasset* is a right to, or an interest in, such a *specified investment* by operation of article 89 (Rights to or interests in investments); and (b) would be a *qualifying cryptoasset* if article 88F(4)(a) to (c) of the *Regulated Activities Order* were disregarded.
specified investment cryptoasset firm	an *authorised person* who: (a) has a *Part 4A permission* to carry on a *regulated activity* other than a *regulated cryptoasset activity*; and (b) carries on an activity under that *permission* in relation to *specified investment cryptoassets*.
stablecoin backing assets	*assets* received or held by *firm* in its capacity as trustee under *CASS* 16.5.2R for the benefit of the *holders* of a *qualifying stablecoin* in respect of which that *firm* is the *qualifying stablecoin issuer*.
stablecoin backing funds	*money* received or held by a *firm* in its capacity as trustee under *CASS* 16.5.2R for the benefit of the *holders* of a *qualifying stablecoin* in respect of which that *firm* is the *qualifying stablecoin issuer*.
stablecoin pool	a number ('X') of *qualifying stablecoins* calculated in accordance with *CASS* 16.2.8R.
stablecoin QCDD	a *QCDD* produced in relation to a *UK qualifying stablecoin*.
supplementary disclosure document	a document which is a supplementary disclosure document for the purposes of Chapter 1 (Qualifying cryptoasset public offers and admissions to trading) of Part 2 (Markets in cryptoassets: designated activities) of the *Cryptoassets Regulations*.
third-party custodian	(a) a *person* who is authorised and supervised in the *UK* or in a *third country* for the activity of safeguarding for

	the account of another *person* of *assets* including *core backing assets* (excluding *on-demand deposits*) and *expanded backing assets*; or (b) any *person* appointed to safeguard *core backing assets* (excluding *on-demand deposits*) or *expanded backing assets* in circumstances described in *CASS* 16.6.7R(2).
transparency crypto intermediary	a *firm dealing in qualifying cryptoassets as principal* when trading in *qualifying cryptoassets* otherwise than on a matched principal basis.
transparency reporting firm	a *firm* that is either: (a) a *UK QCATP operator*; or (b) a *transparency crypto intermediary*, to which *CRYPTO* 7 applies.
UK QCATP	a *qualifying cryptoasset trading platform*, the operation of which requires *authorisation*.
UK QCATP operator	the operator of a *UK QCATP*.
UK qualifying cryptoasset execution venue	a *qualifying cryptoasset execution venue*, the operation of which requires *authorisation*.
UK qualifying stablecoin	a *qualifying stablecoin* issued by a *firm* (F): (a) in respect of which F is *issuing a qualifying stablecoin*; and (b) where F has a *Part 4A permission* to carry on the activity in (a).
wrapped token	a qualifying cryptoasset ('A') which: (a) relates to an underlying *qualifying cryptoasset* ('B'), where B is *minted* on a blockchain other than one on which A is used ('C'); and (b) is created specifically for the purpose of enabling B to be used on C.

Amend the following definitions as shown.

acknowledgement letter	…

	(2)	…
	(3)	(in *CASS* 16) a *backing asset pool acknowledgement letter* (a letter in the form of the template in *CASS* 16 Annex 1).
acknowledgement letter fixed text	…	
	(4)	…
	(5)	(in *CASS* 16) the text in the template *acknowledgement letter* in *CASS* 16 Annex 1 that is not in square brackets.
acknowledgement letter variable text	…	
	(4)	…
	(5)	(in *CASS* 16) the text in the template *acknowledgement letter* in *CASS* 16 Annex 1 that is in square brackets.
admission to trading	…	
	(2A)	…
	(2B)	(in *CRYPTO*) admission of a *qualifying cryptoasset* to trading on a *UK QCATP*.
	…	
advertisement	(1)	(except in *CRYPTO*) has the meaning in regulation 3 of the *Public Offers and Admissions to Trading Regulations* – in summary, a communication which:
	…	
	(2)	(in *CRYPTO)* has the meaning in regulation 3 (Interpretation: qualifying cryptoasset public offers and admissions to trading) of the *Cryptoasset Regulations* – in summary, a communication which:
		(a) relates to:
		(i) a specific *offer of a qualifying cryptoasset to the public*; or
		(ii) an admission, or proposed admission, of a *qualifying cryptoasset* to trading on a *qualifying cryptoasset trading platform*;

(b) aims specifically to promote the potential *buying* of, or subscribing for, a *qualifying cryptoasset*; and

(c) is not a *QCDD* or *supplementary disclosure document*.

agreeing to carry on a regulated activity the *regulated activity*, specified in article 64 of the *Regulated Activities Order* (Agreeing to carry on specified kinds of activity), of agreeing to carry on an activity specified in Part II, Part 3A, or Part 3B of that Order other than:

…

(aa) …

(ab) *issuing a qualifying stablecoin*;

(ac) *operating a qualifying CATP*;

…

algorithmic trading (1) (except in *CRYPTO* 4.7 and *CRYPTO* 4.8) trading in *financial instruments* which meets the following conditions:

…

(2) (in *CRYPTO* 4.7 and *CRYPTO* 4.8) trading in *qualifying cryptoassets* or *related instruments* which meets the following conditions:

(a) where a computer algorithm automatically determines individual parameters of orders, such as whether to initiate the order, the timing, price or quantity of the order for how to manage the order after its submission; and

(b) there is limited or no human intervention; but

does not include any system that is only used for the purpose of routing orders to one or more *qualifying cryptoasset trading platforms* or *trading venues* (as applicable) or the processing of orders involving no determination of any trading parameters or for the confirmation of orders or the post-trade processing of executed transactions.

approved bank (1) (except in *COLL* ~~and~~, *CASS* 15 and *CASS* 16) (in relation to a *bank* account opened by a firm):

…

…

(3) …

(4) (in *CASS* 16) (in relation to a *backing funds account* opened by a *firm*):

(a) the *central bank* of a state that is a member of the *OECD* ('an *OECD* state');

(b) a *credit institution* that is supervised by the *central bank* or other banking regulator of an *OECD* state; and

(c) any *credit institution* that:

(i) is subject to regulation by the banking regulator of a state that is not an *OECD* state;

(ii) is required by the law of the country or territory in which it is established to provide audited accounts;

(iii) has minimum net assets of £5 million (or its equivalent in any other currency at the relevant time);

(iv) has a surplus of revenue over expenditure for the past 2 financial years; and

(v) has an annual report which is not materially qualified.

asset …

(2) …

(3) (in *CRYPTO* and *CASS* 16) any property, right, entitlement or interest, excluding *money*.

client …

(B) in the *FCA Handbook*:

(1) (except in *PROF*, in *MIFIDPRU* 5, in relation to a *credit-related regulated activity*, in relation to *regulated funeral plan activity*, in relation to a *home finance transaction* ~~and~~, in relation to *insurance risk transformation* and activities directly arising from *insurance risk transformation*, and in relation to *issuing a qualifying stablecoin* in *PRIN* and *SYSC* 15A) has the meaning given in *COBS* 3.2, that is (in summary and without prejudice to the detailed effect of *COBS* 3.2) a *person* to whom a *firm* provides, intends to provide or has provided a service in the course of carrying on a *regulated activity*, or in the case of *MiFID or equivalent third country business*, an *ancillary service*:

…

…

(12) …

(13) (in *PRIN* and *SYSC* 15A in relation to *issuing a qualifying stablecoin*):

(a) a *person* to whom a *firm* provides, intends to provide or has provided a service in the course of carrying on a *regulated activity*; and

(b) where not otherwise included in (a), the *holder* of a *qualifying stablecoin* which is issued by a *qualifying stablecoin issuer*.

client money …

(2A) (in *MIFIDPRU*, *FEES*, *CASS* 6, *CASS* 7, *CASS* 7A and *CASS* 10 and, in so far as it relates to matters covered by *CASS* 6, *CASS* 7~~,~~ and *COBS* ~~and *IPRU(INV)* 11~~) subject to the *client money rules*, *money* of any currency:

…

(b) that, in the course of carrying on *designated investment business* that is not *MiFID business* or *issuing a qualifying stablecoin*, a *firm* holds for a *client*; or

…

…

complaint …

(2) (in *DISP*, except *DISP* 1.1 and (in relation to *collective portfolio management*) in the *consumer awareness rules*, the *complaints handling rules*, the *complaints record rule*, and in *CONRED* 5, *CONRED* 6, *CREDS* 9, in *SUP* 12 ~~and,~~ in *SUP* 15 and in *SUP* 16) any oral or written expression of dissatisfaction, whether justified or not, from, or on behalf of, a *person* about the provision of, or failure to provide, a financial service, *claims management service* or a *redress determination*, which:

…

…

controlled activity (in accordance with section 21(9) of the *Act* (The classes of activity and investment)) any of the following activities specified in Part 1 of Schedule 1 to the Financial Promotions Order (Controlled Activities):

…

(ia) …

(ib) safeguarding cryptoassets (paragraph 7A);

(ic) operating a qualifying cryptoasset trading platform (paragraph 7B);

(id) arranging qualifying cryptoasset staking (paragraph 7C);

CRD credit institution (1) (except in *COLL* ~~and,~~ *FUND* and *CASS* 16) a *credit institution* that has its registered office (or, if it has no registered office, its head office) in the *UK*, excluding an *institution* to which the *CRD* does not apply under the *UK* provisions which implemented article 2 of the *CRD* (see also *full CRD credit institution*).

(2) (in *COLL* ~~and,~~ *FUND* and *CASS* 16) a *credit institution* that:

…

customer …

(B) in the *FCA Handbook*:

(1) (except in relation to *SYSC* 19F.2, *ICOBS*, *retail premium finance*, a *credit-related regulated activity*, *regulated claims management activity*, *regulated funeral plan activity*, *regulated pensions dashboard activity*, *MCOB* 3A, an *MCD credit agreement*, *CASS* 5, for the purposes of *PRIN* in relation to *MiFID or equivalent third country business* and *issuing a qualifying stablecoin*, *DISP* 1.1.10-BR, *PROD* 1.4 and *PROD* 4) and in relation to *payment services* and issuing *electronic money* (where not a *regulated activity*) a *client* who is not an *eligible counterparty* for the relevant purposes.

…

(10) …

(11) (in *PRIN* in relation to *issuing a qualifying stablecoin*) a *client* who is not an *eligible counterparty* for the relevant purposes.

data protection legislation

(1) (except in *CRYPTO* 4) the General Data Protection Regulation (EU) No 2016/679 and the Data Protection Act 2018.

(2) (in *CRYPTO* 4) has the same meaning as in section 3 (Terms relating to the processing of personal data) of the Data Protection Act 2018.

designated investment

…

(4) …

(5) (in *COBS*) in addition and to the extent it does not fall within (1):

(a) a *qualifying cryptoasset*; and

(b) a *relevant specified investment cryptoasset*.

designated investment business

(1) (except in *COMP*) any of the following activities, specified in Part II of the *Regulated Activities Order* (Specified Activities), which is carried on by way of business:

…

(t) …

(u) *issuing a qualifying stablecoin* (article 9M (Issuing qualifying stablecoin));

(v) *safeguarding cryptoassets* (article 9N(1)(a) (Safeguarding of qualifying cryptoassets and relevant specified investment cryptoassets));

(w) *arranging cryptoasset safeguarding* (article 9N(1)(b));

(x) *operating a qualifying CATP* (article 9S (Operating a qualifying cryptoasset trading platform));

(y) *dealing in qualifying cryptoassets as principal* (article 9T (Dealing in qualifying cryptoassets as principal)), but disregarding the exclusion in article 9U (Article 9T exclusion: absence of holding out etc.);

(z) *dealing in qualifying cryptoassets as agent* (article 9W (Dealing in qualifying cryptoassets as agent));

(za) *arranging deals in qualifying cryptoassets* (article 9Y (Arranging deals in qualifying cryptoassets)); and

(zb) *arranging qualifying cryptoasset staking* (article 9Z6 (Qualifying cryptoasset staking)).

(2) (in *COMP*) any of the activities falling within (1) except:

(a) *issuing a qualifying stablecoin* (article 9M);

(b) *safeguarding cryptoassets* (article 9N(1)(a));

(c) *arranging cryptoasset safeguarding* (article 9N(1)(b));

(d) *operating a qualifying CATP* (article 9S);

(e) *dealing in qualifying cryptoassets as principal* (article 9T), but disregarding the exclusion in article 9U;

(f) *dealing in qualifying cryptoassets as agent* (article 9W);

(g) *arranging deals in qualifying cryptoassets* (article 9Y); and

(h) *arranging qualifying cryptoasset staking* (article 9Z6).

eligible counterparty business

the following services and activities carried on by a *firm*:

(a) *dealing on own account*, *execution of orders on behalf of clients* or reception and transmission of orders; ~~or~~

(b) any *ancillary service* directly related to a service or activity referred to in (a); ~~or~~

(c) …

(d) *dealing in qualifying cryptoassets as principal*;

(e) *dealing in qualifying cryptoassets as agent*;

(f) *arranging deals in qualifying cryptoassets*;

(g) *arranging qualifying cryptoasset staking*;

(h) *issuing a qualifying stablecoin*;

(i) *safeguarding cryptoassets*; or

(j) *arranging cryptoasset safeguarding*.

execution of orders on behalf of clients

(1) (except in *CRYPTO* and *CRYPTOPRU*) acting to conclude agreements to buy or sell one or more *financial instruments* on behalf of *clients*, including the conclusion of agreements to sell *financial instruments* issued by an *investment firm* or a *credit institution* at the moment of their issuance.

…

(2) (in *CRYPTO* and *CRYPTOPRU*) acting to conclude agreements to buy or sell one or more *qualifying cryptoassets* on behalf of *clients*, including the conclusion of agreements to sell *qualifying cryptoassets* issued by a *firm* at the moment of their issuance.

forward-looking statement	(1)	(in *PRM*) has the same meaning as in paragraph 10(2) of Schedule 2 to the *Public Offers and Admissions to Trading Regulations*.
	(2)	(in *CRYPTO* 3) has the same meaning as in paragraph 8(2) ("Protected forward-looking statement") of Part 2 (Further exemption relating to forward-looking statement) of Schedule 2 (Compensation: exemptions) to the *Cryptoassets Regulations*.
holder	…	
	(b)	…
	(c)	(in relation to a *qualifying stablecoin*):
		(i) the *person* who has the right to *redeem* that *qualifying stablecoin*; or
		(ii) a *person* who is exercising the right in (i) until *redemption* is completed in respect of that *qualifying stablecoin*.

[*Editor's note*: The definition of 'market maker' takes into account the changes introduced by the Short Selling Rules Sourcebook Instrument 2026, which comes into force on 13 July 2026, and the Commodity Derivatives (Ancillary Activity Exemption) Instrument 2025 (FCA 2025/61), which comes into force on 1 January 2027.]

market maker	…	
	(5)	…
	(6)	(in *CRYPTO*) a *person* who holds themselves out on a *qualifying CATP* on a continuous basis as being willing to *deal* in *qualifying cryptoassets* as *principal* by buying and selling *qualifying cryptoassets* against that *person's* proprietary capital at prices defined by that *person*.
material change	(in *COBS* 11 and *CRYPTO* 5.4) a significant event that could impact parameters of best execution, such as cost, price, speed, likelihood of execution and settlement, size, nature or any other consideration relevant to the execution of the order.	
over the counter	(1)	(except in *CRYPTO*) (in relation to a transaction in an *investment*) not *on-exchange*.
	(2)	(in *CRYPTO*) in relation to a transaction in *qualifying cryptoassets* not on a *UK QCATP*.

periodic statement (1) (except in *CRYPTO*) a report which a *firm* is required to provide to a *client* pursuant to:

…

(2) (in *CRYPTO*) a report which a *firm* is required to provide to a *client* pursuant to *CRYPTO* 9.

personal transaction a trade in a *designated investment* or *qualifying cryptoasset*, or in *COBS* 11.7A only, a trade in a *financial instrument*, effected by or on behalf of a *relevant person*, where at least one of the following criteria are met:

…

proprietary trading (in *SYSC* 27 (Senior managers and certification regime: (Certification regime) and *COCON*) *dealing in investments as principal* as part of a business of trading in *specified investments*. For these purposes *dealing in investments as principal* includes:

(a) any activities that would be included but for the exclusion in Article 15 (Absence of holding out etc.), Article 16 (Dealing in contractually based investments) or, for a *UK AIFM* or *UK UCITS management company*, article 72AA (Managers of UCITS and AIFs) of the *Regulated Activities Order*;

(b) *dealing in qualifying cryptoassets as principal*; and

(c) any activities that would be included in (b) but for the exclusion in article 9U (Article 9T exclusion: absence of holding out etc.) of the *Regulated Activities Order*.

protected forward-looking statement (1) (in *PRM*) a *forward-looking statement* that satisfies the conditions set out in *PRM* 8.1.3R.

(2) (in *CRYPTO* 3) a *forward-looking statement* that satisfies the conditions set out in *CRYPTO* 3.7.3R.

qualifying cryptoasset (1) (as defined in ~~paragraph 26F (Qualifying cryptoasset) of Schedule 1 to the *Financial Promotion Order*~~ article 88F (Qualifying cryptoasset) of *Regulated Activities Order*):

~~(1)~~ ~~Any cryptoasset (other than a cryptoasset fall in (2))~~
(a) A *cryptoasset* which is:

~~(a)~~ (i) fungible; ~~and~~

~~(b)~~ (ii) transferable~~.~~;

(iii) not solely a record of value or contractual rights, including rights in another *cryptoasset*; and

(iv) not excluded by (c).

(b) For the purposes of (1)(a)(ii), the circumstances in which a *cryptoasset* is to be treated as 'transferable' include where it confers transferable rights.

~~(2)~~ (c) A ~~cryptoasset~~ *cryptoasset* does not fall within ~~(1)~~ (1)(a) if it is:

~~(a)~~ (i) ~~a *controlled investment* falling within any of paragraphs 12 to 26E or, so far as relevant to any such *investment*, paragraph 27 of Schedule 1 to the *Financial Promotion Order*;~~ a *specified investment cryptoasset*, other than one specified by:

(A) article 74A (Electronic money) of the *Regulated Activities Order*; or

(B) article 88F (Qualifying cryptoassets) of the *Regulated Activities Order*;

~~(b)~~ (ii) ~~electronic money (as defined in regulation 2(1) (Interpretation) of the *Electronic Money Regulations*)~~ *electronic money*;

~~(c)~~ (iii) ~~fiat currency~~ currency of the *United Kingdom* or any other country or territory, including a central bank digital currency; or

~~(d) fiat currency issued in digital form; or~~

~~(e)~~ (iv) a ~~cryptoasset~~ *cryptoasset* that:

~~(i)~~ (A) cannot be transferred or sold in exchange for ~~money~~ *money* or other ~~cryptoassets~~ *cryptoassets*, except by way of redemption with the issuer; and

~~(ii)~~ (B) can only be used ~~in a limited way and meets one of the following conditions~~ by the holder to:

(1) ~~it allows the holder to~~ acquire goods or services ~~only~~ from the issuer; or

(2) ~~it is issued by a professional issuer and allows the holder to~~ acquire goods or services ~~only~~ within a limited network of service providers which have direct commercial agreements with the issuer~~; or~~.

~~(3) it may be used only to acquire a very limited range of goods or services.~~

~~(3) For the purposes of this definition, a cryptoasset is any cryptographically secured digital representation of value or contractual rights that:~~

~~(a) can be transferred, stored or traded electronically; and~~

~~(b) uses technology supporting the recording or storage of data (which may include distributed ledger technology).~~

(2) (insofar as referring to the *controlled investment*, in accordance with article 2 (Interpretation: general) of the *Financial Promotion Order*) has the meaning given by article 88F (Qualifying cryptoassets) of the *Regulated Activities Order*, except that the condition as to the *cryptoasset* being transferable is to be taken as met if a communication made in relation to the *cryptoasset* describes it as being:

(a) transferable; or

(b) conferring transferable rights.

redemption …

(2) …

(3) (in relation to a *qualifying stablecoin*) the process by which a *qualifying stablecoin issuer* fulfils its obligation to the *holder* of a *qualifying stablecoin*, whether carried out directly or indirectly (for example, through a third party), to provide value in exchange for the *holder* returning a *qualifying stablecoin*.

regulated activity …

(B) in the *FCA* Handbook:

(1) (in accordance with section 22 of the *Act* (Regulated activities)) the activities specified in Part II (Specified activities), Part 3A (Specified activities in relation to information) and Part 3B (Claims management activities in Great Britain) of the *Regulated Activities Order*, which are, in summary:

…

(aa) …

(ab) *issuing a qualifying stablecoin* (article 9M (Issuing qualifying stablecoin));

(ac) *safeguarding cryptoassets* (article 9N(1)(a) (Safeguarding of qualifying cryptoassets and relevant specified investment cryptoassets));

(ad) *arranging cryptoasset safeguarding* (article 9N(1)(b));

(ae) *operating a qualifying CATP* (article 9S (Operating a qualifying cryptoasset trading platform));

(af) *dealing in qualifying cryptoassets as principal* (article 9T (Dealing in qualifying cryptoassets as principal));

(ag) *dealing in qualifying cryptoassets as agent* (article 9W (Dealing in qualifying cryptoassets as agent));

(ah) *arranging deals in qualifying cryptoassets* (article 9Y (Arranging deals in qualifying cryptoassets));

(ai) *arranging qualifying cryptoasset staking* (article 9Z6 (Qualifying cryptoasset staking));

…

(2) in *DISP*, except *DISP* 1.1, *DISP* 1.2, *DISP* 1.3 and *DISP* 1.9: (in accordance with the *FCA's* power under section 226 of the *Act*) all of the activities included in (B)(1) as at ~~6 April 2026~~ 25 October 2027, unless expressly excluded in *DISP* 2.3.1R.

relevant person …

(1) …

(1A) (in *CRYPTO* 4) (in accordance with regulation 17(4) (Interpretation: market abuse in qualifying cryptoassets and related instruments) of the *Cryptoassets Regulations*) a *person*, in relation to a *relevant qualifying cryptoasset* or *related instrument*, who is:

(a) a *relevant issuer* of that *relevant qualifying cryptoasset* or *related instrument*;

(b) a *person responsible for the offer* of that *relevant qualifying cryptoasset* or *related instrument*;

(c) a *UK QCATP operator* in relation to a *relevant qualifying cryptoasset*; or

(d) a *relevant dealer in principal*.

…

restricted mass market investment any of the following:

…

(e) a *qualifying cryptoasset* other than one which is part of a *qualifying stablecoin product* that includes a *UK qualifying stablecoin*;

…

retail customer …

(2) (in *PRIN* and *COCON*):

…

(g) …

(h) where a *firm* is a *qualifying stablecoin issuer*, a *customer* who is not a *professional client*.

…

retail investor (1) (in *GEN*, *COBS*, *COLL*, *DISC* and the Investment Funds sourcebook) a *person* meeting the criteria in *DISC* 1A.1.5R.

(2) (in *CRYPTO* 3) a *person* who is not a 'qualified investor' as defined by paragraph 9 of Part 2 (Supplementary provisions relating to Part 1) of Schedule 1 (Exceptions

from prohibition of offers to the public) to the *Cryptoassets Regulations*.

retail market business the *regulated activities* and *ancillary activities* to those activities, *payment services*, issuing *electronic money*, and activities connected to the provision of *payment services* or issuing of *electronic money*, of a *firm* in a distribution chain (including a *manufacturer* and a *distributor*) which involves a *retail customer*, but not including the following activities:

…

(6) *insurance distribution activities* carried on by a *firm* in respect of a *group policy* that:

…

(c) do not involve any direct contact between the *firm* and that *person*~~.~~; and

(7) the activities specified as designated activities under section 71K (Designated activities) of the *Act* by regulations 7 (Designated activities: public offers of qualifying cryptoassets) and 8 (Designated activities: admissions to trading on a qualifying cryptoasset trading platform) of the *Cryptoassets Regulations*, where:

(a) the carrying on of those activities would involve the carrying on of *regulated activities* or *ancillary activities* to those activities; and

(b) those activities are carried on in relation to a *qualifying cryptoasset* that is not a *UK qualifying stablecoin*.

specified investment (1) any of the following *investments* specified in Part III of the *Regulated Activities Order* (Specified Investments):

…

(p) *rights to or interests in investments* (article 89)~~.~~;

(r) a *qualifying cryptoasset* (article 88F); and

(s) a *qualifying stablecoin* (article 88G).

…

third country firm (1) (in *SYSC*) either:

…

(2) (in *COBS* and *DISP*) a *firm* which operates from an establishment in the *United Kingdom* and which:

(a) if it is a body corporate or a partnership, is formed or incorporated under the law of a *third country*; or

(b) if not a body corporate or partnership, operates from a principal place of business in a *third country*.

[*Editor's note*: The definition of 'working day' takes into account the changes made by the Commodity Derivatives (Position Limits, Position Management and Perimeter) Instrument 2025 (FCA 2025/4), which comes into force on 6 July 2026, the Short Selling Rules Sourcebook Instrument 2026 (FCA 2026/16), which comes into force on 13 July 2026, and the Notification of Third Party Arrangements and Operational Incident Reporting Instrument 2026 (FCA 2026/6), which comes into force on 18 March 2027.]

working day	(1)	(in *PRM*, *MAR* 5-A, *MAR* 9 ~~and~~, *MAR* 10 and *CRYPTO* 3) (as defined in section 103 of the *Act*) any day other than a Saturday, a Sunday, Christmas Day, Good Friday or a day which is a bank holiday under the Banking and Financial Dealings Act 1971 in any part of the *United Kingdom*.
	…	

CRYPTOASSETS (INTERMEDIARIES) 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 137A (The FCA's general rules);
(b) section 137T (General supplementary powers); and
(c) section 139A (Power of the FCA to give guidance); and

(2) 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 Consequentials) 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 (Intermediaries) 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 5, after CRYPTO 4 (Cryptoasset market abuse).

5 Execution and orders

5.1 Application

General application

5.1.1 R This chapter applies to a *firm*:

(1) *dealing in qualifying cryptoassets as principal*;

(2) *dealing in qualifying cryptoassets as agent*; and

(3) *arranging deals in qualifying cryptoassets*.

5.1.2 R *CRYPTO* 5.8 applies to a *firm* carrying out *qualifying cryptoasset activities* except a *firm* which only carries out the *regulated activity* of *issuing a qualifying stablecoin*.

5.1.3 G Certain provisions in this chapter require *firms* to provide *clients* with information 'in good time'. *Guidance* on the provision of information 'in good time' can be found in *COBS* 1.4.2G.

5.1.4 R This chapter does not apply to a *firm* in relation to its *eligible counterparty business*.

5.1.5 R This chapter does not apply to *redemption* of a *UK qualifying stablecoin* where such *redemption* is undertaken by a third party appointed in accordance with *CRYPTO* 2.

5.2 Execution venues for retail clients

5.2.1 R This section applies where a *firm* is:

(1) executing orders; or

(2) *arranging deals in qualifying cryptoassets*,

for a *retail client* or *elective professional client* who is not an *overseas retail client* or *overseas elective professional client*.

Firm obligations

5.2.2 R A *firm* must ensure that, when executing orders or receiving and transmitting orders for execution for a *client*, the order is executed on a *UK qualifying cryptoasset execution venue*.

5.2.3 R Where a *firm* is otherwise *arranging deals in qualifying cryptoassets*, it must take all reasonable steps to ensure that the arrangements it provides only result in a *client's* order to be executed on a *UK qualifying cryptoasset execution venue*.

5.2.4 G (1) The *rule* in *CRYPTO* 5.2.3R applies to *firms* which are *arranging deals in qualifying cryptoassets* for a *retail client* where multiple *firms* may be providing arrangements.

(2) Where there are multiple *firms* involved in providing arrangements for a *retail client's* order to be executed, *CRYPTO* 5.2.3R requires each *firm* to take all reasonable steps to ensure that the arrangements it provides only result in a *client's* order being executed on a *UK qualifying cryptoasset execution venue*.

5.2.5 G (1) Where a *firm* executes *client* orders on a matched principal basis, the *firm* is not deemed to be a *qualifying cryptoasset execution venue* when only acting in that capacity to execute the orders.

(2) However, where a *firm* otherwise acts in the capacity of *principal* when executing *client* orders, it should be considered as the *qualifying cryptoasset execution venue*.

5.2.6 R Where a *firm* (A) is *dealing in qualifying cryptoassets as principal* and executes orders for *clients*, it must not systematically or predominantly source liquidity from a *QCATP* where the operator of that *QCATP*:

(1) is not *authorised* as a *UK QCATP operator*; and

(2) is in the same *group* as A.

5.2.7 R A *firm* must make and retain written records of how it continues to satisfy itself that it fulfils the requirements in this section.

5.3 Admission to trading requirement for intermediaries offering services

Admission to trading requirements for qualifying cryptoassets

5.3.1 R This section applies where a *firm* is:

(1) *dealing in qualifying cryptoassets (as principal or agent)*; or

(2) *arranging deals in qualifying cryptoassets*,

for, or with, a *retail client* who is not an *overseas retail client*.

5.3.2 R A *firm* must not *deal* in *qualifying cryptoassets* or *arrange deals in qualifying cryptoassets* for or with a *client* unless either of the following conditions are met:

(1)

(a) the *qualifying cryptoasset* is available to be traded by *retail clients* on a *UK QCATP* and is *admitted to trading* on a *retail UK QCATP* in compliance with *CRYPTO* 3;

(b) the *UK QCATP operator* has made available the *QCDD* and (where relevant) *supplementary disclosure document* for the *qualifying cryptoasset* in accordance with *CRYPTO* 3; and

(c) the *qualifying cryptoasset* has not been withdrawn from trading on all *UK QCATPs*; or

(2) the *firm* is *arranging deals in qualifying cryptoassets* and:

(a) arranges the sale of a *qualifying cryptoasset* offered on condition that the *qualifying cryptoasset*:

(i) will be available to be traded by *retail clients*; and

(ii) will be *admitted to trading* on a *retail UK QCATP*; and

(b) the *UK QCATP* has made available the *QCDD* and (where relevant) *supplementary disclosure document* for the *qualifying cryptoasset* in accordance with *CRYPTO* 3.

5.3.3 R *CRYPTO* 5.3.2R does not apply to *UK qualifying stablecoins*.

5.3.4 G Where a *firm* offers a trading pair of *qualifying cryptoassets*, either of the conditions in *CRYPTO* 5.3.2R must be fulfilled for both *qualifying cryptoassets* unless the *rule* in *CRYPTO* 5.3.6R applies.

5.3.5 G The *rule* in *CRYPTO* 5.3.6R sets out an exclusion to the *rule* in *CRYPTO* 5.3.2R.

5.3.6 R Where a *qualifying cryptoasset* which had been *admitted to trading* has been withdrawn from trading on all *retail UK QCATPs*, a *firm* may purchase the *qualifying cryptoasset* from a *client* or arrange for a *client* to *sell* their *qualifying cryptoassets* to another *person* except to a *retail client*.

5.3.7 R (1) A *firm* must make available to *clients* the *QCDD* and (where relevant) *supplementary disclosure documents* for the *qualifying cryptoassets* it deals or arranges deals in before the *client*'s initiation of the transaction.

(2) A *firm* must make available to *clients* the *stablecoin QCDD* for the *UK qualifying stablecoins* that it deals or arranges deals in before the *client*'s initiation of the transaction.

5.3.8 G In *CRYPTO* 5.3.2R and *CRYPTO* 5.3.7R, the documents may be made available by providing a link to where the documents are published in accordance with *CRYPTO* 2 and *CRYPTO* 3.

5.3.9 R Where a *firm* (A) is *arranging deals in qualifying cryptoassets*, it is not required to make the *QCDD*, *stablecoin QCDD* or *supplementary disclosure documents* available in accordance with *CRYPTO* 5.3.7R where:

(1) the arrangements provided by A require a *client* to engage with another *firm* (B) for the transaction to take place; and

(2) B complies with the *rule* in *CRYPTO* 5.3.7R.

5.3.10 G The *rule* in *CRYPTO* 5.3.9R is to avoid duplication of requirements where there are multiple *firms* involved in a transaction. Where *CRYPTO* 5.3.9R applies, *firms* should take all reasonable steps to ensure that the *client* will be provided with the documents specified in *CRYPTO* 5.3.7R by another *firm* before the *client*'s initiation of the transaction.

5.3.11 R A *firm* must make and retain written records of how it continues to satisfy itself that it fulfils the requirements in this section.

5.4 Execution and order handling rules

Obligation to execute orders on terms most favourable to the client

5.4.1 R (1) A *firm* must take all sufficient steps to obtain, when executing orders, the best possible results for its *clients*, taking into account the *execution factors*.

(2) The *execution factors* to be taken into account are price, costs, speed, likelihood of execution and settlement, size, nature or any other consideration relevant to the execution of an order.

5.4.2 G The obligation on *firms* in *CRYPTO* 5.4.1R is subject to the requirements in *CRYPTO* 5.2.2R and *CRYPTO* 5.2.6R.

5.4.3 G *CRYPTO* 5.4.1R(1) does not apply to a *firm* when it engages in *matched principal trading* for the purpose of executing *client* orders on a *UK QCATP* it operates, when acting in accordance with the non-discretionary rules of the *UK QCATP*.

Application of best execution obligation

5.4.4 G *CRYPTO* 5.4.1R applies where a *firm* owes contractual or agency obligations to the *client*.

5.4.5 G A *firm* executing orders on behalf of a *client* when *dealing in qualifying cryptoassets as principal* should be considered as undertaking execution of *client* orders subject to the requirements under this chapter, and in particular, those obligations in relation to best execution.

5.4.6 G A *firm* executing *client* orders on a matched principal basis is subject to the requirements of this chapter in relation to the execution of orders on behalf of *clients*.

5.4.7 G Where a *firm* executes a quote after a *client* accepts it, the *firm* complies with *CRYPTO* 5.4.1R where:

(1) the quote would meet the *firm's* obligations under *CRYPTO* 5.4.1R if the *firm* executed the quote at the time it was provided; and

(2) the quote is not manifestly out of date, taking into account:

(a) the changing market conditions; and

(b) the time elapsed between the offer and acceptance of the quote.

5.4.8 G The obligation to deliver the best possible result when executing *client* orders applies in relation to all types of *qualifying cryptoassets*. However, given the differences in characteristics of *qualifying cryptoassets*, it may be difficult to identify and apply a uniform standard of, and procedure for, best execution that would be valid and effective for all groups (or categories) of *qualifying cryptoassets*. Best execution obligations should therefore be applied to take into account the different circumstances surrounding the execution of orders for particular types of *qualifying cryptoassets*.

Best execution criteria

5.4.9 R (1) A *firm* must, when executing *client* orders, take into account the following criteria for determining the relative importance of the *execution factors*:

(a) the characteristics of the *client*, including the categorisation of the *client* as retail or professional;

(b) the characteristics of the *client* order;

(c) the characteristics of *qualifying cryptoassets* that are the subject of that order; and

(d) the characteristics of the *qualifying cryptoasset execution venues* to which that order can be directed.

(2) A *firm* satisfies the *qualifying cryptoasset best execution obligation* to the extent that it executes an order or a specific aspect of an order following specific instructions from the *client* relating to that order or the specific aspect of that order.

(3) A *firm* must not structure or charge its commissions in such a way as to discriminate unfairly between *qualifying cryptoasset execution venues*.

(4) A *firm* must, when executing orders or taking decisions to deal *qualifying cryptoassets over the counter*, check the fairness of the price proposed to the *client*:

(a) by gathering market data used in the estimation of the price of such product; and

(b) where possible, by comparing with similar or comparable transactions.

Role of price

5.4.10 R Where a *firm* executes an order on behalf of a *retail client*, the best possible result must be determined in terms of the total consideration, representing the price of the *qualifying cryptoasset* and the costs related to execution. This must include:

(1) all expenses incurred by the *client* that are directly related to the execution of the order, including *qualifying cryptoasset execution venue* fees, gas fees and settlement fees; and

(2) any other fees paid to third parties involved in the execution of the order.

5.4.11 G When a *firm* executes a *retail client's* order in the absence of specific *client* instructions, for the purposes of ensuring that the *firm* obtains the best possible result for the *client*, the *firm* should take into consideration all factors that will enable it to deliver the best possible result in terms of the total consideration, representing the price of the *qualifying cryptoasset* and the costs related to execution.

5.4.12 G The following factors may be given precedence over the immediate price and cost consideration in *CRYPTO* 5.4.10R only insofar as they are instrumental in delivering the best possible result in terms of the total consideration to the *retail client*:

(1) speed;

(2) likelihood of execution;

(3) likelihood of settlement;

(4) the size and nature of the order; or

(5) any other implicit transaction costs.

Following specific instructions from a client

5.4.13 R Whenever there is a specific instruction from a *client*, a *firm* must execute the order following the specific instruction.

5.4.14 G When a *firm* executes an order following specific instructions from the *client*, it should be treated as having satisfied its best execution obligations only in respect of the part or aspect of the order to which the *client* instructions relate. The fact that the *client* has given specific instructions which cover one part or aspect of the order should not be treated as releasing

the *firm* from its best execution obligations in respect of any other parts or aspects of the *client* order that are not covered by such instructions.

5.4.15 G A *firm* should not induce a *client* to instruct it to execute an order in a particular way, by expressly indicating or implicitly suggesting the content of the instruction to the *client*, when the *firm* ought reasonably to know that an instruction to that effect is likely to prevent it from obtaining the best possible result for that *client*. However, this should not prevent a *firm* from inviting a *client* to choose between 2 or more specified *qualifying cryptoasset execution venues*, provided that those *qualifying cryptoasset execution venues* are consistent with the execution policy of the *firm*.

Delivering best execution where there are competing qualifying cryptoasset execution venues

5.4.16 R A *firm's* own commissions and the costs for executing an order in each of the eligible *qualifying cryptoasset execution venues* must be taken into account when assessing and comparing the results that would be achieved for a *client* by executing the order on each of the *qualifying cryptoasset execution venues* listed in the *firm's* execution policy that is capable of executing that order.

5.4.17 G The obligation to deliver best execution for a *retail client* where there are competing *qualifying cryptoasset execution venues* is not intended to require a *firm* to:

(1) compare the results that would be achieved for its *client* on the basis of its own execution policy and its own commissions and fees with results that might be achieved for the same *client* by any other *firm* on the basis of a different execution policy or a different structure of commissions or fees; or

(2) compare the differences in its own commissions which are attributable to differences in the nature of the services that the *firm* provides to *clients*.

5.4.18 G A *firm* would be considered to structure or charge its commissions in a way which discriminates unfairly between *qualifying cryptoasset execution venues* if:

(1) it charged a different commission or spread to *clients* for execution on different *qualifying cryptoasset execution venues*; and

(2) that difference did not reflect actual differences in the cost to the *firm* of executing on those venues.

5.4.19 G The provisions of this section which provide that costs of execution include a *firm's* own commission or fees charged to the *client* for the provision of an investment service should not apply for the purpose of determining which *qualifying cryptoasset execution venues* must be included in the *firm's* execution policy in accordance with *CRYPTO* 5.4.23R.

5.4.20 R A *firm* must not receive any remuneration, discount or non-monetary benefit for routing *client* orders to a particular *qualifying cryptoasset execution venue* which would infringe the requirements on conflicts of interests as set out in *SYSC* 10 or inducements as set out in *COBS* 2.3 (for *firms* carrying on business other than *MiFID, equivalent third country or optional exemption business*).

5.4.21 G *Firms* should also consider the *rules* and *guidance* set out in *CRYPTO* 5.7 in respect of any remuneration, discount or non-monetary benefit for routing *client* orders.

Requirement for order execution arrangements including an order execution policy

5.4.22 R A *firm* must establish and implement effective arrangements for complying with the obligation to take all sufficient steps to obtain the best possible results for its *clients*. In particular, the *firm* must establish and implement an order execution policy to allow it to obtain, in accordance with *CRYPTO* 5.4.1R, the best possible result for the execution of *client* orders.

5.4.23 R (1) The order execution policy in *CRYPTO* 5.4.22R must include, in respect of each group (or category) of *qualifying cryptoassets*, information on the different *qualifying cryptoasset execution venues* where the *firm* executes its *client* orders and the factors affecting the choice of *qualifying cryptoasset execution venue*.

(2) The policy referred to in (1) must at least include those *qualifying cryptoasset execution venues* that enable the *firm* to obtain on a consistent basis the best possible result for the execution of *client* orders.

5.4.24 R (1) A *firm* must provide appropriate information to its *clients* on its order execution policy.

(2) The information referred to in (1) must:

(a) explain clearly how orders will be executed by the *firm* for the *clients*; and

(b) include sufficient details and be provided in a way that can be easily understood by *clients*.

5.4.25 R A *firm* must obtain the prior consent of its *clients* to its order execution policy.

5.4.26 R (1) Where a *firm's* order execution policy provides for the possibility that *client* orders may be executed outside a *UK QCATP*, the *firm* must, in particular, inform its *clients* about that possibility.

(2) A *firm* must obtain the express prior consent of its *clients* before proceeding to execute their orders outside a *UK QCATP*.

(3) A *firm* may obtain the consent referred to in (2) either in the form of a general agreement or in respect of individual transactions.

Execution policies

5.4.27 R (1) A *firm* must review its order execution policy and order execution arrangements:

(a) at least on an annual basis; and

(b) upon occurrence of a *material change* that affects the *firm's* ability to continue to obtain the best possible result for the execution of its *client* orders on a consistent basis using the venue included in its execution policy,

and, as part of such review, the *firm* must consider making changes to the relative importance of the *execution factors* in meeting its *qualifying cryptoasset best execution obligation*.

(2) The information on the order execution policy must be customised depending on the group (or category) of *qualifying cryptoassets* and type of the service provided and must include the information set out in (3) to (9).

(3) A *firm* must provide *clients*, in a *durable medium* (or by means of a website, mobile application or any other digital medium, in accordance with the *website conditions*, to the extent it is not a *durable medium*), with the following details on its execution policy in good time prior to the provision of the service:

(a) in compliance with *CRYPTO* 5.4.9R(1), an account of the relative importance the *firm* assigns to the *execution factors*, or the process by which the *firm* determines the relative importance of those factors;

(b) a list of the *qualifying cryptoasset execution venues* on which the *firm* places significant reliance in meeting its *qualifying cryptoasset best execution obligation* and specifying which *qualifying cryptoasset execution venues* are used for each group (or category) of *qualifying cryptoassets* for *retail client* orders and *professional client* orders;

(c) a list of factors used to select a *qualifying cryptoasset execution venue*, including:

(i) qualitative factors such as settlement arrangements, *client* protection measures, operational resilience,

transparent disclosures, or any other relevant consideration, and

(ii) the relative importance of each factor,

ensuring that the information about the factors used to select a *qualifying cryptoasset execution venue* for execution is consistent with the controls used by the *firm* to demonstrate to *clients* that best execution has been achieved on a consistent basis when reviewing the adequacy of the *firm's* policy and arrangements;

(d) how the *execution factors* of price costs, speed, likelihood of execution and any other relevant factors are considered as part of all sufficient steps to obtain the best possible result for the *client*;

(e) where applicable:

(i) that the *firm* executes orders outside a *UK QCATP*;

(ii) any additional risks arising from execution outside a *UK QCATP*; and

(iii) upon *client* request, additional information about any additional risks of this means of execution;

(f) a clear and prominent warning that any specific instruction from a *client* may prevent the *firm* from taking the steps that it has designed and implemented in its order execution policy to obtain the best possible result for the execution of those orders in respect of the elements covered by those instructions; and

(g) a summary of:

(i) the selection process for *qualifying cryptoasset execution venues*;

(ii) execution strategies employed;

(iii) the procedures and process used to analyse the quality of execution obtained; and

(iv) how the *firm* monitors and verifies that the best possible results were obtained for *clients*.

(4) Where a *firm* applies different fees depending on the *qualifying cryptoasset execution venue*, the *firm* must explain these differences in sufficient detail in order to allow the *client* to understand the advantages and the disadvantages of the choice of a single *qualifying cryptoasset execution venue*.

(5) Where a *firm* invites *clients* to choose a *qualifying cryptoasset execution venue*, it must provide fair, clear and not misleading information to prevent the *client* from choosing one *qualifying cryptoasset execution venue* rather than another on the sole basis of the price policy applied by the *firm*.

(6) A *firm* must only receive third-party payments that comply with the *rules* in *COBS* 2.3 and must inform *clients* about the inducements that the *firm* may receive from the *qualifying cryptoasset execution venues*. The information must specify the fees charged by the *firm* to all counterparties involved in the transaction and, where the fees vary depending on the *client*, the information must indicate the maximum fees or range of the fees that may be payable.

(7) Where a *firm* charges more than one participant in a transaction, in compliance with the *rules* in *COBS* 2.3, the *firm* must inform its *client* of the value of any monetary or non-monetary benefits received by the *firm*.

(8) Where a *client* makes reasonable and proportionate requests to a *firm* for information about its policies or arrangements and how they are reviewed, the *firm* must answer clearly and within a reasonable time.

(9) Where a *firm* executes orders for *retail clients*, it must provide those *clients* with a summary of the relevant policy, focused on the total cost they incur.

5.4.28 G (1) When establishing its order execution policy in accordance with *CRYPTO* 5.4.22R, a *firm* should determine the relative importance of the factors mentioned in *CRYPTO* 5.4.1R, or at least establish the process by which it determines the relative importance of these factors, so that it can deliver the best possible result to its *clients*.

(2) Ordinarily, the *FCA* would expect that price will merit a high relative importance in obtaining the best possible result for *professional clients*. However, in some circumstances for some *clients*, orders, *qualifying cryptoassets* or markets, the policy may appropriately determine that other *execution factors* are more important than price in obtaining the best possible execution result.

5.4.29 G A *firm* should apply its order execution policy to each *client* order that it executes with a view to obtaining the best possible result for the *client* in accordance with that policy.

5.4.30 G The obligation to take all sufficient steps to obtain the best possible result for the *client* should not be treated as requiring a *firm* to include in its order execution policy all available *qualifying cryptoasset execution venues*.

5.4.31 G A *firm* executing orders should be able to include a single *qualifying cryptoasset execution venue* in its policy only where it is able to show that this allows it to obtain best execution for its *clients* on a consistent basis. *Firms* should select a single *qualifying cryptoasset execution venue* only where they can reasonably expect that the selected *qualifying cryptoasset execution venue* will enable them to obtain results for *clients* that are at least as good as the results that they could reasonably expect from using alternative *qualifying cryptoasset execution venues*. This reasonable expectation should be supported by relevant data or by other internal analyses conducted by *firms*.

5.4.32 G The provisions of this section relating to a *firm's* order execution policy are without prejudice to the general obligation of a *firm* to monitor the effectiveness of its order execution arrangements and policy and assess the *qualifying cryptoasset execution venues* in its order execution policy on a regular basis.

5.4.33 R (1) A *firm* must monitor the effectiveness of its order execution arrangements and execution policy to identify and, where appropriate, correct any deficiencies.

(2) In particular, a *firm* must assess, on a regular basis, whether the *qualifying cryptoasset execution venues* included in its order execution policy provide for the best possible result for the *client* or whether it needs to make changes to its execution arrangements, taking into account relevant data or other internal analyses conducted by *firms*.

(3) The *firm* must notify *clients* of any *material changes* to its order execution arrangements or order execution policy.

5.4.34 R (1) A *firm* must be able to demonstrate to its *clients*, at their request, that it has executed their orders in accordance with its order execution policy.

(2) A *firm* must be able to demonstrate to the *FCA*, upon request, its compliance with *CRYPTO* 5.4.1R and with the related provisions in this chapter which require *firms* to execute orders on terms most favourable to the *client*.

5.4.35 G In order to obtain the best execution for a *client*, a *firm* should compare and analyse relevant data.

Duty of portfolio managers, receivers and transmitters to act in the client's best interest

5.4.36 G The provisions of this section are relevant to:

(1) a portfolio manager that deals in *qualifying cryptoassets* on behalf of *client*, in particular, when *dealing in qualifying cryptoassets as agent*

or *arranging deals in qualifying cryptoassets*, in accordance with its mandate when carrying out *portfolio management* services; or

(2) a *firm* which receives and transmits orders in *qualifying cryptoassets* to other *persons* for execution as part of *arranging deals in qualifying cryptoassets*.

5.4.37 R (1) A *firm* that provides *portfolio management* services must comply with the *client's best interests rule* when transmitting orders to other *persons* for execution that result from decisions by the *firm* to deal in *qualifying cryptoassets* on behalf of its *client*.

(2) A *firm* that receives and transmits orders for execution in *qualifying cryptoassets* must comply with the *client's best interests rule* when transmitting *client* orders to other *persons* for execution.

(3) In order to comply with the *client's best interests rule* under (1) or (2), a *firm* must comply with (4) to (9).

(4) A *firm* must take all sufficient steps to obtain the best possible result for its *client*, taking into account the *execution factors*, the relative importance of which must be determined by reference to:

(a) the criteria set out in *CRYPTO* 5.4.9R(1); and

(b) for *retail clients*, *CRYPTO* 5.4.10R.

(5) A *firm* satisfies its obligations under (1) or (2), and is not required to take the steps mentioned in (4), to the extent that it follows specific instructions from its *client* when transmitting an order to another entity for execution.

(6) A *firm* must establish and implement a policy that enables it to comply with (4). The policy must identify, in respect of each group (or category) of *qualifying cryptoassets*, the *persons* with which the orders are placed or to which the *firm* transmits orders for execution. The *persons* identified must have execution arrangements that enable the *firm* to comply with its obligations under this *rule* when it places or transmits orders to that *person* for execution.

(7) A *firm* must:

(a) provide information to its *clients* on the policy in (6) and its order execution policy established in accordance with *CRYPTO* 5.4.27R(2) to (9);

(b) provide *clients* with appropriate information about the *firm* and its services and the *persons* chosen for execution; and

(c) upon reasonable request from a *client*, provide its *clients* or potential *clients* with information about entities where the orders are transmitted or placed for execution.

(8) A *firm* must:

(a) monitor on a regular basis the effectiveness of its policy established in accordance with (6) including, in particular, the execution quality of the entities identified;

(b) where deficiencies in the effectiveness have been identified, correct any deficiencies in its order execution policy where appropriate;

(c) review its order execution policy and order execution arrangements at least annually and whenever a *material change* occurs that affects the *firm's* ability to continue to obtain the best possible result for its *clients*; and

(d) assess whether a *material change* has occurred and consider making changes to the *execution venues* or *persons* on which it places significant reliance in meeting its *qualifying cryptoasset best execution obligation*.

(9) A *firm* must, when executing orders or taking decisions to deal *qualifying cryptoassets over the counter*, check the fairness of the price proposed to the *client*, by gathering market data used in the estimation of the price of such product and, where possible, by comparing with similar or comparable transactions.

5.4.38 G This section is not intended to require a duplication of effort as to best execution between a *firm* which receives and transmits orders for execution or *portfolio management* and any *firm* to which that *firm* transmits its orders for execution.

5.4.39 G (1) A *firm* transmitting orders to other entities for execution may select a single entity for execution only where:

(a) it can show that this provides the best possible result for its *clients* on a consistent basis; and

(b) it can reasonably expect that the selected entity will enable it to obtain results for *clients* that are at least as good as the results that could reasonably be expected from using alternative entities for execution.

(2) This reasonable expectation referred to in (1)(b) should be supported by relevant data or by other internal analyses conducted by the *firm*.

Minimum number of price sources

5.4.40 G (1) In complying with its *qualifying cryptoasset best execution obligation*, a *firm* should check, where available, at least 3 reliable price sources from *UK qualifying cryptoasset execution venues*.

(2) Where a *UK QCATP* makes the prices publicly available, the *firm* should prioritise checking these prices.

(3) Where there are fewer than 3 *UK qualifying cryptoasset execution venues* that can execute the order, the *firm* should at least check the prices on the available *UK qualifying cryptoasset execution venues*.

5.4.41 G The *guidance* in *CRYPTO* 5.4.40 is not intended to:

(1) require a *firm* to execute a *client* order on the *qualifying cryptoasset execution venues* it has checked;

(2) require a *firm* to include the *qualifying cryptoasset execution venues* that it checks prices on in its order execution policy; or

(3) prevent a *firm* from considering prices on a non-*UK qualifying cryptoasset venue* provided that such a venue meet the equivalent standards of governance, operational integrity and *market abuse* controls.

5.4.42 G Circumstances where the *guidance* in *CRYPTO 5*.4.40 is not expected to be relevant include where:

(1) a *firm* is engaged in the activity of *qualifying cryptoasset lending or borrowing*; or

(2) a transaction involves exchanging a *UK qualifying stablecoin* for:

(a) another *UK qualifying stablecoin*; or

(b) fiat money; or

(3) a transaction involves an exchange of 2 *qualifying cryptoassets* (A and B):

(a) at a fixed ratio; and

(b) where the economic value of A and B is the same.

5.4.43 G An example of a transaction in *CRYPTO* 5.4.42G(3) is issuing or redeeming a *wrapped token*.

5.5 Pre-trade disclosures to clients

Disclosure of firm role

5.5.1 R A *firm* must disclose its role(s) to *retail clients* or *professional clients* before executing *client* orders, including whether it acts as a *principal* or *agent* for each order.

5.5.2 G Where a *firm* is acting in a matched principal capacity for an order, the *firm* should make this clear to the *client* before executing each order.

5.5.3 G The disclosure in *CRYPTO* 5.5.1R can take a standard format covering multiple orders or types of orders if the *firm* always acts in the same capacity for such orders or types of orders.

Price disclosure

5.5.4 R *CRYPTO* 5.5.7R to *CRYPTO* 5.5.10G apply where a *firm* is *dealing in qualifying cryptoassets as principal* for a *retail* or *professional client*.

5.5.5 R *CRYPTO* 5.5.7R(1) and (2), *CRYPTO* 5.5.8R, *CRYPTO* 5.5.9R and *CRYPTO* 5.5.10G do not apply:

(1) when a *firm* engages in *matched principal trading* for the purpose of executing *client* orders on a *UK QCATP* it operates, when acting in accordance with the non-discretionary rules of the *UK QCATP*; or

(2) to a transaction which involves an exchange of 2 *qualifying cryptoassets* (A and B):

(a) at a fixed ratio; and

(b) where the economic value of A and B is the same.

5.5.6 G An example of a transaction in *CRYPTO* 5.5.5R is issuing or redeeming a *wrapped token*.

5.5.7 R A *firm* must disclose the following to its *client* prior to execution of the *client's* order:

(1) a firm price at which the order can be executed;

(2) the duration of the time period for which the *firm* can execute the order at that price; and

(3) any fees or charges for the execution of the order.

5.5.8 R Where a *client* has accepted the price within the time period disclosed by the *firm*, the *firm* must execute the order at that price or at a price that is more advantageous to the *client*.

5.5.9 R Where the price is no longer available for execution due to exceptional circumstances, the *firm*:

(1) is not required to execute the order at the price accepted by the *client*;

(2) must inform the *client* why the order was not executed; and

(3) must seek fresh instructions from the *client*.

5.5.10 G The *FCA* expects that exceptional circumstances in respect of *CRYPTO* 5.5.9R will be rare occurrences, but may include such circumstances as extreme market volatility.

Settlement

5.5.11 R A *firm* must clearly inform the *client* of the process for the settlement of *qualifying cryptoasset* transactions it deals or arranges in, including any associated risks, as applicable.

5.5.12 G Where a *firm* provides the service of arranging or otherwise bringing about settlement of a *qualifying cryptoasset* transaction, the *FCA* expects the *firm* to:

(1) initiate the final settlement of the transaction within 24 hours of the transaction being executed;

(2) have previously disclosed the nature of the service to its *client*; and

(3) have recorded this in accordance with *COBS* 8.1, in the case of a *retail client*.

5.6 Client order handling

General principles

5.6.1 R (1) A *firm* which is carrying out *client* orders must implement procedures and arrangements which provide for the prompt, fair and expeditious execution of *client* orders, relative to other orders or the trading interests of the *firm*.

(2) These procedures or arrangements in (1) must allow for the execution of otherwise comparable orders in accordance with the time of their reception by the *firm*.

Carrying out client orders

5.6.2 R A *firm* must, when carrying out *client* orders:

(1) ensure that orders executed on behalf of *clients* are promptly and accurately recorded and allocated;

(2) carry out otherwise comparable *client* orders sequentially and promptly unless the characteristics of the order or prevailing market conditions make this impracticable, or the interests of the *client* require otherwise; and

(3) inform a *retail client* about any material difficulty relevant to the proper carrying out of orders promptly upon becoming aware of the difficulty.

5.6.3 G For the purposes of this section, orders should not be treated as otherwise comparable if they are received by different media and it would not be practicable for them to be treated sequentially.

Use of information relating to pending client orders

5.6.4 R A *firm* must not misuse information relating to pending *client* orders and must take all reasonable steps to prevent the misuse of such information by any of its *relevant persons*.

Aggregation and allocation of orders

5.6.5 R A *firm* must not carry out a *client* order or a transaction for own account in aggregation with another *client* order unless the following conditions are met:

(1) it is unlikely that the aggregation of orders and transactions will work overall to the disadvantage of any *client* whose orders are to be aggregated;

(2) it is disclosed to each *client* whose order is to be aggregated that the effect of aggregation may work to its disadvantage in relation to a particular order; and

(3) the *firm* has established and effectively implemented an order allocation policy, which provides for the fair allocation of aggregated orders and transactions, including how the volume and price of orders determine allocations and the treatment of partial executions.

Partial execution of aggregated client order

5.6.6 R Where a *firm* aggregates an order with one or more other *client* orders and the aggregated order is partially executed, it must allocate the related trades in accordance with its order allocation policy.

Aggregation and allocation of transactions for own account

5.6.7 R A *firm* which has aggregated transactions for own account with one or more *client* orders must not allocate the related trades in a way that is detrimental to a *client*.

5.6.8 R (1) Where a *firm* aggregates a *client* order with a transaction for own account and the aggregated order is partially executed, it must allocate the related trades to the *client* in priority to the *firm*.

(2) Where the *firm* is able to demonstrate on reasonable grounds that without the combination it would not have been able to carry out the order on such advantageous terms, or at all, it may allocate the transaction for own account proportionally, in accordance with its order allocation policy referred to in *CRYPTO* 5.6.5R(3).

5.6.9 R As part of the order allocation policy referred to in *CRYPTO* 5.6.5R(3), a *firm* must put in place procedures to prevent the reallocation, in a way that is detrimental to the *client*, of transactions for own account which are executed in combination with *client* orders.

5.6.10 G For the purposes of this section, the reallocation of transactions should be considered as detrimental to a *client* if, as an effect of that reallocation, unfair precedence is given to the *firm* or to any particular *person*.

5.6.11 G In this section, carrying out *client* orders includes:

(1) the *execution of orders on behalf of clients*;

(2) the transmission of orders to other entities for execution that result from decisions to deal in *qualifying cryptoassets* on behalf of *clients* when providing the service of *portfolio management*; and

(3) the transmission of *client* orders to other entities for execution when providing the service of reception and transmission of orders.

5.7 Conflicts of interest during order execution

5.7.1 G This section sets out requirements in relation to managing conflicts of interest where a *firm* executes orders for a *client*. In addition to the *qualifying cryptoasset best execution obligation* and the *rules* in this section, *firms* are also reminded of other relevant obligations in *PRIN*, *SYSC* and *COBS* relating to conflicts of interest, acting in the *client's* best interests, and restrictions on inducements, as applicable.

5.7.2 G Where a *firm* is executing orders for *qualifying cryptoassets* for *clients*, arrangements that involve accepting or demanding monetary or non-monetary benefits for routing *client* orders to a *qualifying cryptoasset execution venue* risk breaching:

(1) the *qualifying cryptoasset best execution obligation*; and

(2) obligations in *PRIN*, *SYSC* and *COBS* relating to:

(a) conflicts of interest;

(b) acting in the *client's* best interests; and

(c) the restrictions on inducements.

Functional separation requirement

5.7.3 G As set out in *SYSC*, a *firm* must maintain and operate effective organisational and administrative arrangements with a view to taking all reasonable steps to prevent conflicts of interest from adversely affecting the interests of its *clients* when executing orders or receiving and transmitting for execution orders for a *client* for *qualifying cryptoassets*. This includes segregating, within its own operating environment, tasks and responsibilities which may be regarded as incompatible with each other, or which may generate systematic conflicts of interest.

5.7.4 G *Firms* should design their systems to address any *client* detriment arising out of conflicts between the *firm's qualifying cryptoasset* proprietary trading operations and *client* execution operations.

5.7.5 G Appropriate systems are expected to include functional separation between a *firm's* proprietary trading operations and client execution operations. Functional separation includes but is not limited to:

(1) transparent and appropriately segregated lines of responsibility between the *firm's* different operations;

(2) clear and separate reporting lines between the *firm's* different operations or business lines;

(3) defined roles for management functions, including risk, compliance and audit functions; and

(4) established *information barriers* between *persons* and different parts of the business.

5.8 Personal account dealing

5.8.1 R A *firm* that conducts *qualifying cryptoasset activity* must establish, implement and maintain adequate arrangements aimed at preventing the activities in *CRYPTO* 5.8.2R in the case of any *relevant person* who:

(1) is involved in activities that may give rise to a conflict of interest; or

(2) has access to:

(a) inside information as defined in the *Cryptoassets Regulations*; or

(b) other confidential information relating to *clients* or transactions with or for *clients*,

by virtue of an activity carried out by them on behalf of the *firm*.

5.8.2 R The activities to which *CRYPTO* 5.8.1R applies are:

(1) entering into a *personal transaction* which meets at least one of the following criteria:

(a) that *person* is prohibited from entering into it under Part 2 of Chapter 2 of the *Cryptoassets Regulations*;

(b) it involves the misuse or improper disclosure of the confidential information in *CRYPTO* 5.8.1R(2); or

(c) it conflicts or is likely to conflict with an obligation of the *firm* to a *customer* under the *regulatory system* or any other obligation of the *firm* under the *Cryptoassets Regulations*;

(2) advising or procuring, other than in the proper course of their employment or contract for services, any other *person* to enter into a transaction in a *qualifying cryptoasset* or *related instrument* which, if a *personal transaction* of the *relevant person*, would be covered by (1) or a relevant provision; and

(3) disclosing, other than in the normal course of their employment or contract for services, any information or opinion to any other *person* if the *relevant person* knows, or reasonably ought to know, that as a result of that disclosure that other *person* will or would be likely to:

(a) enter into a transaction in a *qualifying cryptoasset* or *related instrument* which, if a *personal transaction* of the *relevant person*, would be covered by (1) or a relevant provision; or

(b) advise or procure another *person* to enter into such a transaction.

5.8.3 R For the purposes of this section, the relevant provision is *CRYPTO* 5.6.4R.

5.8.4 R The requirements of this section are without prejudice to the prohibition under regulation 24 of the *Cryptoassets Regulations*.

Dealing

5.8.5 R The arrangements required under this section must be designed to ensure that:

(1) each *relevant person* covered by this section is aware of the restrictions on *personal transactions*, and of the measures established by the *firm* in connection with *personal transactions* and disclosure, in accordance with this section; and

(2) the *firm*:

(a) is informed promptly of any *personal transaction* entered into by a *relevant person*, either by notification of that transaction or by other procedures enabling the *firm* to identify such transactions; or

(b) in the case of *outsourcing* arrangements, ensures that the service provider to which the activity is *outsourced* maintains a record of *personal transactions* entered into by

any *relevant person* and provides that information to the *firm* promptly on request; and

(3) a record is kept of the *personal transaction* notified to the *firm* or identified by it, including any authorisation or prohibition in connection with such a transaction.

Disapplication of rule on personal account dealing

5.8.6 R This section does not apply to *personal transactions* effected under a discretionary portfolio management service where there is no prior communication in connection with the transaction between the portfolio manager and the *relevant person* or other *person* for whose account the transaction is executed.

5.8.7 R For the purposes of this section, a *person* who is not a director, partner or equivalent, or manager of the *firm* will only be a *relevant person* to the extent that they are involved in the provision of *qualifying cryptoasset activity*.

Successive personal transactions

5.8.8 R Where successive *personal transactions* are carried out on behalf of a *person* in accordance with prior instructions given by that *person*, the obligations under this section do not apply:

(1) separately to each successive transaction if those instructions remain in force and unchanged; or

(2) to the termination or withdrawal of such instructions, provided that any *qualifying cryptoassets* or *related instruments* which had previously been acquired pursuant to the instructions are not disposed of at the same time as the instructions terminate or are withdrawn.

5.8.9 R Obligations under this section do apply in relation to a *personal transaction*, or the commencement of successive *personal transactions*, that are carried out on behalf of the same *person* if those instructions are changed or if new instructions are issued.

5.9 Records

5.9.1 R A *firm* must make and keep records evidencing its compliance with this chapter.

5.9.2 R A record made and kept by a *firm* in accordance with this chapter must be:

(1) provided by the *firm* to the *FCA* upon request; and

(2) kept for a period of 5 years or, where requested by the *FCA*, for a period of up to 7 years.

CRYPTOASSETS (TRADING PLATFORMS, TRANSPARENCY AND RECORDS) 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 137A (The FCA's general rules);
(b) section 137T (General supplementary powers); and
(c) section 139A (Power of the FCA to give guidance); and

(2) 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 Consequentials) 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 (Trading Platforms, Transparency and Records) Instrument 2026.

By order of the Board
25 June 2026

Annex

Amendments to the Cryptoassets sourcebook (CRYPTO)

In this Annex, all the text is new and is not underlined.

Insert the following new chapters, CRYPTO 6, CRYPTO 7 and CRYPTO 8, after CRYPTO 5 (Execution and orders).

6 Cryptoasset trading platforms

6.1 Purpose and application

Purpose

6.1.1 G The purpose of this chapter is to set out requirements relating to the *operation of a qualifying CATP*. This chapter does not apply to bilateral systems, which are excluded from the *qualifying CATP* definition.

Application

6.1.2 R This chapter applies to a *UK QCATP operator*.

6.2 Trading process requirements

Rules, procedures and arrangements

6.2.1 R A *firm* must implement, publish and maintain clear and transparent operating rules for a *UK QCATP* it operates, including at least:

(1) objective, non-discriminatory rules and proportionate criteria for:

(a) ensuring fair and orderly trading on; and

(b) promoting fair and open access to,

the *UK QCATP* for users;

(2) objective criteria for the efficient execution of orders that are established and implemented in non-discretionary rules;

(3) arrangements for the sound management of the technical operations of the *UK QCATP*, including effective contingency arrangements to cope with the risks of systems disruption;

(4) transparent rules regarding the criteria for determining the *qualifying cryptoassets* that can be traded on or under its systems and regarding their withdrawal from *admission to trading*;

(5) non-discriminatory and objective criteria governing access to its *UK QCATP* and that must provide that users of that platform:

(a) are of sufficient good repute;

(b) have a sufficient level of trading ability, competence and experience;

(c) where applicable, have adequate organisational arrangements; and

(d) have sufficient financial resources to trade on the platform; and

(6) arrangements to:

(a) monitor compliance with its rules by users of the *UK QCATP*; and

(b) suspend or terminate the provision of access to a *UK QCATP* for a user in the case of any non-compliance with its rules.

6.2.2 R (1) A *firm* must publish information on the operating rules for its trading platform free of charge and in a manner that:

(a) is easily accessible, non-discriminatory, prominent, comprehensible, fair, clear and not misleading; and

(b) facilitates all users' understanding.

(2) The information in (1) must include an explanation of any:

(a) trading limits; and

(b) adverse consequences arising from breaches of the operating rules.

(3) A *firm* must provide access to its operating rules to all of its users at all times.

Admission, suspension and withdrawal

6.2.3 R (1) A *firm* must ensure that, on a *UK QCATP* it operates, a *UK retail investor* is only able to trade directly in *qualifying cryptoassets admitted to trading* in accordance with *CRYPTO* 3.

(2) A *firm* that *admits to trading* a *qualifying cryptoasset* (A):

(a) on a *UK QCATP* it operates (B); and

(b) where trading in A is limited to designated categories of investors,

must ensure that only investors to whom (b) applies can trade in A on B.

(3) A *firm* must direct its users to the *QCDD* and (where relevant) *supplementary disclosure document relating* to A.

(4) The disclosure in (3) must be made prior to trading in a manner that:

(a) is easily accessible, non-discriminatory, prominent, comprehensible, fair, clear and not misleading; and

(b) facilitates all users' understanding.

6.2.4 R (1) A *firm* that wishes to *admit to trading*, on a *UK QCATP* it operates, a *qualifying cryptoasset*:

(a) of which it is the issuer;

(b) for which it has arranged the issue; or

(c) in which it otherwise has a financial interest,

must disclose the nature of its interest in that *qualifying cryptoasset* in the relevant *QCDD* and (where relevant) *supplementary disclosure document* provided to users of the *UK QCATP*.

(2) A *firm* must have in place policies and procedures to mitigate the conflict in (1), including functional separation of individuals engaged in:

(a) the issuance process; and

(b) the *admission to trading* process,

in the case of the *qualifying cryptoasset* to which (1) applies.

(3) A *firm* must be able to demonstrate that the arrangements in (2) allow for the independent performance of the *admission to trading* process.

(4) A *firm* must make a disclosure on its website if, following *admission to trading*, it acquires a financial interest in a *qualifying cryptoasset* it has *admitted to trading*.

6.2.5 R (1) If a *firm* withdraws a *qualifying cryptoasset* from trading on a *UK QCATP*, it must, prior to doing so, notify the fact and consequences of withdrawal to the public through appropriate direct channels.

(2) If a *firm* withdraws a *UK qualifying stablecoin* from trading on a *UK QCATP*, it must, prior to doing so, in addition to (1), notify the issuer and the *FCA*.

6.2.6 R Where a *firm* has withdrawn a *qualifying cryptoasset* from trading on a *UK QCATP* it operates, it must update its website and the *FCA-owned centralised repository* with a notice duly dated comprising:

(1) the date of withdrawal;

(2) the *digital token identifier*;

(3) the *UK QCATP operator* name and *LEI*;

(4) the name of the *person* who obtained *admission to trading* and that person's *LEI*, where available; and

(5) an explanation of the reasons for withdrawal.

6.2.7 G A *firm* withdraws a *qualifying cryptoasset* from trading on a *UK QCATP* it operates, for the purposes of *CRYPTO* 6.2.6R, both when it withdraws a *qualifying cryptoasset* from trading altogether and where the *qualifying cryptoasset* ceases to be available to a class of investors, such as *retail investors*.

6.2.8 R (1) A *firm* must maintain a record on its website of all *qualifying cryptoassets admitted to trading* on a *UK QCATP* it operates.

(2) The record in (1) must:

(a) be kept up to date;

(b) identify whether the relevant *qualifying cryptoasset* is available to be traded by *UK retail investors*;

(c) comprise details of the *QCDD* and (where relevant) *supplementary disclosure document* that correspond to a *qualifying cryptoasset*; and

(d) be easily accessible and comprehensible to users of the *UK QCATP*.

Co-location

6.2.9 R Where a *firm* permits co-location in relation to the *UK QCATP*, its rules on co-location services must be transparent, fair and non-discriminatory.

6.3 Systems and controls for UK QCATP operators

Systems and controls

6.3.1 R A *firm* must have arrangements to ensure it is adequately equipped to:

(1) identify all significant risks to its operation;

(2) manage the risks to which it is exposed; and

(3) put in place effective measures to mitigate those risks.

6.3.2 R A *firm* must have in place effective systems, procedures and arrangements to ensure that the trading systems of a *UK QCATP* it operates:

(1) are resilient;

(2) have sufficient capacity to deal with peak order and message volumes;

(3) can ensure orderly trading under conditions of severe market stress;

(4) can reject orders that exceed predetermined volume and price thresholds or are clearly erroneous;

(5) are fully tested having regard to paragraphs (1) to (4);

(6) can halt, suspend or constrain trading;

(7) are subject to effective business continuity arrangements to ensure continuity of platform services if there is any failure of, or disruption to, the trading system;

(8) are designed to prevent market abuse, and to detect it if it occurs; and

(9) are sufficiently robust to prevent their abuse for the purposes of *money laundering* or terrorist financing.

6.3.3 R A *firm* must maintain resources and have back-up facilities in place to enable it to provide *reportable pre-trade transparency information*, where relevant, and *reportable post-trade transparency information*, in accordance with *CRYPTO* 7.

6.3.4 R A *firm* must, with regard to its own interests and those of:

(1) the *UK QCATP*;

(2) its *group*; and

(3) users,

have arrangements to identify clearly and manage any conflict with adverse consequences for the sound functioning of the *UK QCATP*.

6.3.5 G A *firm* is also subject to the conflicts-of-interest requirements in *Principle* 8, *SYSC* 10 and *CRYPTO* 3.

Measures preventing disorderly markets

6.3.6 R A *firm* must have the ability to halt, suspend or constrain trading, on a *UK QCATP* it operates, by a *person*:

(1) trading from an establishment maintained by it; or

(2) habitually resident,

in the *United Kingdom*.

6.3.7 R For the purposes of *CRYPTO* 6.3.6R, and to avoid significant disruptions to the orderliness of trading, a *firm* must calibrate the parameters for halting, suspending or constraining trading in a way that takes into account:

(1) the liquidity of different *qualifying cryptoassets*;

(2) the nature of the *qualifying CATP* market model; and

(3) the types of users,

to ensure the parameters are sufficient to avoid significant disruptions to the orderliness of trading.

6.4 Market making and algorithmic trading

Market makers

6.4.1 R (1) A *firm* must identify, document and monitor users who carry out *market making strategies* on a *UK QCATP* it operates.

(2) Where a *firm* offers an incentive scheme or any other legal, contractual, commercial or other arrangement with *market makers* or other liquidity providers, it must:

(a) document and disclose to users such schemes and arrangements, including the terms of such schemes and arrangements;

(b) ensure that the design and effect of such schemes and arrangements promote fair, orderly and efficient trading on the *UK QCATP*; and

(c) monitor compliance with the terms of such schemes and arrangements.

Algorithmic trading

6.4.2 R A *firm* must make, maintain and publish objective, non-discriminatory rules and proportionate criteria relating to permissible use of algorithms on the *UK QCATP* it operates, as well as specifications on:

(1) types of algorithms;

(2) algorithmic trading thresholds; and

(3) algorithmic trading limits commensurate with the nature of the business and the operating capacity of the *UK QCATP*.

6.4.3 R A *firm* must monitor algorithmic trading activity to:

(1) ensure compliance with its rules relating to *CRYPTO* 6.4.2R; and

(2) prevent market abuse.

6.4.4 R A *firm* must have in place and maintain effective systems, procedures and arrangements to ensure that an algorithmic trading system cannot create, or contribute to, disorderly trading conditions on the *UK QCATP* it operates.

6.4.5 R (1) A *firm* must disclose to its users:

(a) the approach to managing and mitigating potential harms arising out of the use of algorithmic trading techniques; and

(b) the numbers of users engaged in algorithmic trading techniques, in accordance with its rules,

on a *UK QCATP* it operates.

(2) The disclosures in (1) must be made in a manner that:

(a) is easily accessible, non-discriminatory, prominent, comprehensible, fair, clear and not misleading; and

(b) facilitates all users' understanding.

6.5 Information to users

Fee structures

6.5.1 R A *firm* must ensure that its fee structures, including all commissions and gas fees:

(1) are transparent, fair and non-discriminatory; and

(2) do not create incentives to place, modify or cancel orders or to execute transactions in a way that contributes to disorderly trading conditions or market abuse.

Settlement of transactions

6.5.2 R A *firm* must clearly inform its users of the process for the settlement of transactions executed on a *UK QCATP* it operates, including any associated risks.

6.5.3 G A *firm* should initiate the final settlement of a transaction within 24 hours of the transaction being executed on the *UK QCATP* it operates.

User agreement and client disclosures

6.5.4 R A *firm* must clearly disclose in any user agreement the rights of its *client* in respect of any *qualifying cryptoasset* traded by the *client* on a *UK QCATP* in the event of:

(1) a change in the underlying software protocols governing the operation of a *qualifying cryptoasset* traded on the *UK QCATP*; and

(2) the *client* electing to terminate the agreement.

6.6 Business activities

Matched principal trading

6.6.1 R A *firm* must not execute any orders against its proprietary capital on a *UK QCATP* it operates, except where *CRYPTO* 6.6.2R applies.

6.6.2 R A *firm* with the appropriate *permission* may engage in *matched principal trading* for the purpose of executing *client* orders on a *UK QCATP* it operates, when acting in accordance with the non-discretionary rules of the *UK QCATP*.

6.6.3 G *Matched principal trading* does not exclude the possibility of settlement risk and, accordingly, a *firm* should take appropriate steps to minimise this risk.

6.6.4 G The effect of *CRYPTO* 6.6.1R is that a *firm* cannot act as a *market maker* on a *UK QCATP* it operates.

Credit risk exposure

6.6.5 R A *firm* must not offer credit to its *clients*.

Trading as principal outside a UK QCATP

6.6.6 R A *firm* with the appropriate *permission* may execute orders against its proprietary capital or engage in *matched principal trading* outside the *UK QCATP* it operates if it:

(1) makes clear to its *client*, at all times, the capacity in which it is providing services to them and the nature of the service, including when executing orders:

(a) against its proprietary capital; or

(b) by *matched principal trading*; and

(2) maintains effective systems, procedures and arrangements to ensure that conflicts of interest are capable of being promptly identified and are adequately managed.

6.6.7 G For the purposes of *CRYPTO* 6.6.6R, when a *firm* executes orders against its proprietary capital, an appropriate *permission* is the *permitted activity* of *dealing in qualifying cryptoassets as principal*. A *UK QCATP operator* requires this *permission* in addition to carrying on the *permitted activity* of *operating a qualifying CATP*. Where a *UK QCATP operator* wishes only to carry on the additional activity of *matched principal trading*, it requires a *permission* of *dealing in qualifying cryptoassets as principal* subject to a *limitation* restricting that activity to *matched principal trading*.

6.7 Records

6.7.1 R A *firm* must make and keep records evidencing its compliance with this chapter.

6.7.2 R A record made and kept by a *firm* in accordance with *CRYPTO* 6 must be:

(1) provided by the *firm* to the *FCA* upon request; and

(2) kept for a period of 5 years or, where requested by the *FCA*, for a period of up to 7 years.

7 Transparency

7.1 Purpose and application

Purpose

7.1.1 G The purpose of this chapter is to set out the pre-trade and post-trade transparency *rules* applying to the reporting of *qualifying cryptoassets*.

Application

7.1.2 R This chapter applies to a *firm*:

(1) that is:

(a) *dealing in qualifying cryptoassets as principal*; or

(b) a *UK QCATP operator*; and

(2) (for the purposes of *CRYPTO* 7.2) that has average revenue of more than or equal to £10m a year having regard to all its activities, for a period of the 3 previous years, including revenue arising from periods when the business was carried on by or in any predecessor entity.

7.1.3 R A *firm* carrying on a *permitted activity* in *CRYPTO* 7.1.2R(1)(b) must perform the calculation in *CRYPTO* 7.1.2R(2) at 12-*month* intervals.

7.1.4 G A *firm* that operates a *UK QCATP* and to which *CRYPTO* 7.2 applies is a *large CATP operator*.

7.2 Pre-trade transparency

Firm obligations

7.2.1 R This section applies only to a *large CATP operator*.

7.2.2 R A *firm* must, in respect of a *qualifying cryptoasset* traded on a *UK QCATP* it operates, publish adequate information about current bid and offer prices and the depth of trading interests at those prices, for the purposes of achieving efficient price formation and fair evaluation of such a *qualifying cryptoasset*.

7.2.3 R A *firm* publishes adequate information for the purposes of *CRYPTO* 7.2.2R where it publishes the pre-trade transparency information described in the table in *CRYPTO* 7.2.5R.

7.2.4 R A *firm* must publish at least the pre-trade transparency information in *CRYPTO* 7.2.5R on a continuous basis during normal trading hours.

7.2.5 R Table: Pre-trade transparency information to be published, by reference to type of system

	Type of trading system	**Information to be published**	
(1)	Continuous auction order book trading system	The aggregated number of orders and the cryptoassets that those orders represent for at least the 5 best bid and offer price levels of each *qualifying cryptoasset*.	
(2)	Quote-driven trading system	For each *qualifying cryptoasset* traded on the trading system:	
		(a)	the best bid and offer by price of each participant; and
		(b)	the volume corresponding to the price.
(3)	Hybrid trading system	For a hybrid trading system combining different trading systems at the same time, the information in (1) or (2) applicable to each trading system forming that hybrid system.	

(4)	Any other trading system	For each *qualifying cryptoasset* traded on the trading system:	
		(a)	the level of orders or quotes; and
		(b)	the 5 best bid and offer price levels where the characteristics of the price discovery mechanism permit.

Making data available on a reasonable commercial basis

7.2.6 R (1) A *firm* must:

(a) make available *reportable pre-trade transparency information* to the public on a reasonable commercial basis; and

(b) ensure non-discriminatory access to the information in (a).

(2) A *firm* must make available the information in (1) free of charge, in a machine-readable format, 15 minutes after publication.

(3) The requirements in (1) do not apply to a *firm* that makes market data available to the public free of charge.

7.2.7 G A *firm* to which *CRYPTO* 7.2.6R(3) applies is subject to *CRYPTO* 7.2.4R.

Waivers

7.2.8 R A *firm* must publish *pre-trade transparency information* unless it reasonably considers that this does not contribute to:

(1) the achievement of efficient price formation; and

(2) fair evaluation of the relevant *qualifying cryptoassets*.

7.2.9 R A *firm* may only rely on *CRYPTO* 7.2.8R not to publish pre-trade transparency information where publication of such information would adversely affect the trading interests of its *clients*.

7.2.10 R A *firm* must publish the rules or processes it adopts to fulfil *CRYPTO* 7.2.8R and (where relevant) *CRYPTO* 7.2.9R before it implements them.

7.2.11 R In determining an appropriate formula or other mechanism applicable to those orders for which it will not publish *reportable pre-trade transparency information* in accordance with *CRYPTO* 7.2.8R, a *firm* must have regard to at least the following factors:

(1) the level of liquidity in the *qualifying cryptoasset*, including whether there are ready and willing buyers and sellers on a

continuous basis and the number, type and ratio of market participants active in the particular product;

(2) any other objective characteristics of the *qualifying cryptoasset*, including the extent to which it is traded in a standardised or frequent way and the average size of spreads;

(3) any negative effect on the fair and orderly trading of the *qualifying cryptoasset* on the *UK QCATP*; and

(4) the nature and extent of public information that would assist *firms* to fulfil their best execution obligations.

7.2.12 R This section does not apply to:

(1) a transaction when there is an exchange of a *UK qualifying stablecoin* for:

(a) another *UK qualifying stablecoin*; or

(b) fiat money; or

(2) a transaction when there is an exchange of 2 *qualifying cryptoassets* (A and B):

(a) at a fixed ratio; and

(b) where the economic value of A and B is the same.

7.2.13 G An example of a transaction in *CRYPTO* 7.2.12R(2) is redeeming a *wrapped token*.

7.3 Post-trade transparency

Application

7.3.1 R The *rules* in *CRYPTO* 7.3 apply in respect of:

(1) transactions in *qualifying cryptoassets* executed on a *UK QCATP*; or

(2) transactions in *qualifying cryptoassets* executed by a *transparency crypto intermediary* acting in that capacity.

Firm reporting obligations

7.3.2 R Where *CRYPTO* 7.3.1R applies, a *transparency reporting firm* must publish post-trade transparency information about the transaction:

(1) as close to real time as is technically possible; and

(2) in any case within 1 minute of the execution of the relevant transaction.

7.3.3 R (1) A *transparency reporting firm* must publish at least the post-trade transparency information in *CRYPTO* 7.3.4R.

(2) The requirement in (1) does not apply to a *transparency crypto intermediary* where a *UK QCATP operator* is required to publish the information in *CRYPTO* 7.3.4R.

7.3.4 R Table: Post-trade transparency information to be published

	Field identifier	Content to be reported
(1)	Trading date and time	The date and time of execution of the transaction (including the time zone where this is not Coordinated Universal Time (UTC)).
(2)	Cryptoasset identification code	The *digital token identifier*.
(3)	Price	The traded price of the transaction excluding commission, other fees and accrued interest. Where the price is recorded using money, use the major currency unit. Where the *qualifying cryptoasset* is traded based on a currency pair, express the quantity of the quote currency for one unit of the base currency.
(4)	Price currency	The currency in which the trading price for the *qualifying cryptoasset* related to the order is expressed. Where the price of the *qualifying cryptoasset* is expressed in monetary terms and in a currency pair, the currency pair in which the price for the *qualifying cryptoasset* related to the order is expressed must be reported. The first currency code must be that of the base currency, and the second currency code must be that of the quote currency. The quote currency determines the price of one unit of the base currency. *Firms* may use ISO currency codes.

(5)	Quantity	The quantity of *qualifying cryptoassets* executed.
(6)	Execution venue	Identification of the execution venue (*LEI*, where available) where the order was submitted. Where the execution venue uses segment market identifier codes (MICs), use the segment MIC. Where the execution venue does not use segment MICs, use the operating MIC.
(7)	Publication date and time	The date and time of publication of the transaction.

Making data available on a reasonable commercial basis

7.3.5 R (1) A *transparency reporting firm* must:

(a) make available *reportable post-trade transparency information* to the public on a reasonable commercial basis; and

(b) ensure non-discriminatory access to the information in (a).

(2) A *transparency reporting firm* must make available the information in (1) free of charge, in a machine-readable format, 15 minutes after publication.

(3) The requirements in (1) do not apply to a *transparency reporting firm* that makes market data available to the public free of charge.

7.3.6 G A *firm* to which *CRYPTO* 7.3.5R(3) applies is subject to *CRYPTO* 7.3.2R.

Authorised deferred publication

7.3.7 R A *transparency reporting firm* subject to *CRYPTO* 7.3.2R may defer publication of post-trade transparency information for up to 3 months from the date of execution of a transaction only where it considers such deferral to be necessary for the purposes of:

(1) the achievement of efficient price formation; and

(2) fair evaluation of the relevant *qualifying cryptoassets*.

7.3.8 R A *transparency reporting firm* may only rely on *CRYPTO* 7.3.7R to defer publication of post-trade transparency information where publication of such information, in accordance with *CRYPTO* 7.3.2R, would adversely affect the trading interests of its *clients*.

7.3.9 R A *transparency reporting firm* must publish the rules or processes it adopts to fulfil *CRYPTO* 7.3.7R before it implements them.

7.3.10 R In determining the appropriate size thresholds and any other characteristics applicable to those orders for which it will defer publication of *reportable post-trade transparency information* in accordance with *CRYPTO* 7.3.7R:

(1) a *transparency reporting firm* must have regard to at least the factors in *CRYPTO* 7.2.11R; and

(2) a *firm dealing in qualifying cryptoassets as principal* may have regard to its own capacity to offer prices to market participants when publishing hedging transactions it enters in respect of more illiquid or large positions.

7.4 Records

7.4.1 R A *firm* must make and keep a record of the reasons for any determination made under this chapter.

7.4.2 R A record made and kept by a *firm* in accordance with *CRYPTO* 7.4.1R must be:

(1) provided by the *firm* to the *FCA* upon request; and

(2) kept for a period of at least 5 years.

8 Record keeping and reporting: client orders and transactions

8.1 Purpose and application

Purpose

8.1.1 G The purpose of this chapter is to set out the *rules* applying to record keeping and reporting of *client* orders and transactions in *qualifying cryptoassets*.

Application

8.1.2 R This chapter applies to a *firm* that is:

(1) a *UK QCATP operator*;

(2) *dealing in qualifying cryptoassets as principal*;

(3) *dealing in qualifying cryptoassets as agent*; or

(4) *arranging (bringing about) deals in qualifying cryptoassets*.

8.1.3 R This chapter does not apply to the reporting of *qualifying cryptoasset lending or borrowing* transactions.

8.2 Obligation to keep records

8.2.1 R For all *client* orders and all transactions, a *firm* must keep records of the following information, where relevant to that order or transaction:

(1) a *digital token identifier*;

(2) the type of order or transaction as per the *firm's* own specifications;

(3) a buy/sell indicator for the order or transaction;

(4) the quantity of *qualifying cryptoassets* in the order or transaction;

(5) the unit price of the *qualifying cryptoassets* in the order or transaction, excluding commission, other fees and accrued interest;

(6) the reference currency or reference cryptoasset for the price specified in (5);

(7) the total price of the order or transaction (being the sum of the unit price multiplied by the quantity of *qualifying cryptoassets* forming the order or transaction);

(8) the total sum of costs and charges incurred by the *client* in relation to the order or transaction (including gas fees where they apply);

(9) the total consideration for the order or transaction (being the sum of the figures in (7) and (8));

(10) the date and time of placement of the order (expressed in UTC);

(11) the date and time of cancellation of the order (expressed in UTC) and the reason for cancellation;

(12) the date and time of execution of the transaction (expressed in UTC);

(13) the execution venue where the transaction was executed;

(14) a unique identifier for the buyer in the order or transaction;

(15) a unique identifier for the seller in the order or transaction;

(16) a unique identifier for the decision maker responsible for the order within the *firm* placing the order; and

(17) in the case of a transaction settled on-chain:

(a) the transaction hash;

(b) all associated transaction addresses, such as the wallet address and smart contract address; and

(c) network fees.

8.2.2 R A *firm* must determine the person or algorithm taking primary responsibility for the decision required to be recorded under *CRYPTO* 8.2.1R(16) in accordance with predetermined criteria established by that *firm*.

8.2.3 R Where the seller, buyer or decision maker is an individual, the unique identifier included in a record under *CRYPTO* 8.2.1R(14), (15) and (16) must be either:

(1) a national insurance number; or

(2) created using a concatenation of the following elements in the following order:

(a) the date of birth of the individual (in the format YYYYMMDD);

(b) the first 5 characters of the individual's first name; and

(c) the first 5 characters of the individual's surname.

8.2.4 G One or more hash symbols (#) should be appended to first names and surnames shorter than 5 characters to ensure that references to names and surnames in accordance with *CRYPTO* 8.2.3R contain 5 characters.

8.2.5 R Where the seller, buyer or decision maker is not an individual, the unique identifier included in a record must be either:

(1) an *LEI*; or

(2) an alphanumeric code that uniquely identifies the seller, buyer or decision maker.

8.2.6 R Where a *firm* uses the identifier in *CRYPTO* 8.2.5R(2), it must record how that identifier was created and assigned.

8.2.7 R A *firm* must have systems and procedures in place to assess whether it needs to record and retain additional information in relation to *client* orders and transactions to comply with its obligations under the *regulatory system*.

8.2.8 R A record made and kept by a *firm* in accordance with *CRYPTO* 8.2.1R must be:

(1) provided by the *firm* to the *FCA* upon request; and

(2) kept for a period of 5 years from the date of the relevant order or transaction.

8.2.9 G A *firm* should ensure that records are stored in a way accessible for future reference by the *FCA*, in order to enable both the *firm* and the *FCA* to reconstitute each key stage of the processing of each transaction, including settlement.

8.3 Client reporting

Daily reports

8.3.1 R A *firm* must provide a report to each *UK client* on the execution of an order that relates to them. This report must be provided:

(1) promptly; and

(2) at least by the end of the *day* on which:

(a) the order was executed, if executed before the end of the *working day*; or

(b) the information was received by the *firm*, if received before the end of the *working day*.

8.3.2 R A *firm* does not need to provide a report in accordance with *CRYPTO* 8.3.1R where a *client* has agreed in writing they do not want to receive it on this basis.

8.3.3 G Where a *firm* and its *client* agree to proceed in accordance with *CRYPTO* 8.3.2R, the *firm* may provide reports to that *client* on terms to be agreed with that *client*.

Cancellations

8.3.4 R (1) Where an order has been cancelled, a *firm* must provide the *client* with confirmation of, and a reason for, the cancellation.

(2) The information in (1) must be provided promptly and at least by the end of the *day* on which the order was cancelled (if cancelled before the end of the *working day*).

Client requests for information

8.3.5 R A *client* may request, at any time, that a *firm* provide them with the information in *CRYPTO* 8.3.6R, in relation to that *client*:

(1) for all orders (including cancellations);

(2) for the period of 3 years preceding the request; and

(3) in a *durable medium* (or by means of a website, mobile application or any other digital medium in accordance with the *website conditions*, to the extent it is not a *durable medium*),

irrespective of whether they agree with the *firm* not to receive a report in accordance with *CRYPTO* 8.3.1R.

Content of client reports

8.3.6 R The report provided by a *firm* under *CRYPTO* 8.3.1R must include all essential information relating to the execution of the order, including at least the following, as applicable:

(1) the unique identifier used by the *firm* and execution venue (where different) to identify itself when executing that *client's* order;

(2) the unique identifier assigned to the *client* by the *firm* to identify that *client*;

(3) the *digital token identifier* assigned by the *firm* to each *qualifying cryptoasset* involved in the order and transaction (including indicating whether it is available on the Digital Token Identifier Foundation Registry);

(4) an indicator to record whether the *firm* was acting as buyer or seller for the *client* when the order was executed;

(5) the date and time of execution of the order (expressed in UTC);

(6) the quantity of *qualifying cryptoassets* involved in the order;

(7) the unit price the order was executed at;

(8) the total price of the order (being the sum of the unit price multiplied by the quantity of *qualifying cryptoassets* forming the order);

(9) the total sum of all costs and charges incurred by the *client* in relation to the order, including but not limited to:

(a) gas fees;

(b) venue fees;

(c) settlement fees;

(d) any other fees paid to third parties involved in executing the order;

(e) any commission; and

(f) any accrued interest or reward;

(10) the total consideration for the order (being the sum of the figures in (8) and (9)); and

(11) details of any specific instructions given by the client to the *firm* in relation to the order.

8.3.7 R (1) Where information in *CRYPTO* 8.3.6R is readily available on-chain, the *firm* does not need to include this information in the report to the *client*.

(2) Where information is not included in a report to the *client* because it is available on-chain, the *firm* must ensure that the *client* is able to access it.

CRYPTOASSETS (LENDING, BORROWING AND STAKING) 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 137A (The FCA's general rules);
(b) section 137T (General supplementary powers); and
(c) section 139A (Power of the FCA to give guidance); and

(2) 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 Consequentials) 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 (Lending, Borrowing and Staking) Instrument 2026.

By order of the Board
25 June 2026

Annex

Amendments to the Cryptoassets sourcebook (CRYPTO)

In this Annex, all the text is new and is not underlined.

Insert the following new chapters, CRYPTO 9 and CRYPTO 10, after CRYPTO 8 (Record keeping and reporting: client orders and transactions).

9 Cryptoasset lending and borrowing

9.1 Application

Who? What?

9.1.1 R (1) Except as provided for in (2), this chapter applies to an *authorised cryptoasset firm* when providing a *qualifying cryptoasset lending or borrowing* service to a *retail client* who is not an *overseas retail client*.

(2) The requirements in *CRYPTO* 9.4.2R and *CRYPTO* 9.9 apply to an *authorised cryptoasset firm* when providing a *qualifying cryptoasset lending or borrowing* service to a *client* who is not an *overseas client*.

9.1.2 G In this chapter, references to a '*firm*' include circumstances where the *firm* complies with a requirement through arrangements with a third party, such as a *qualifying cryptoasset custodian* or other service provider. In such cases, the *firm* remains responsible for compliance with this chapter and must ensure that its arrangements enable it to meet the relevant requirements.

9.2 Information requirement

9.2.1 R (1) A *firm* must provide a *retail client* with information about the *firm* and its *qualifying cryptoasset lending or borrowing* service.

(2) The information in (1) must be provided to a *retail client*:

(a) each time that *retail client* instructs the *firm* to provide the *qualifying cryptoasset lending or borrowing* service; and

(b) before one of the following, whichever is earlier:

(i) a *retail client* is bound by any agreement relating to *qualifying cryptoasset lending or borrowing*; or

(ii) the provision of those services.

(3) A *firm* must provide the information in (1) in a *durable medium* or via a website, mobile application or any other digital medium that the *firm* may be using in relation to the provision of its *qualifying cryptoasset lending or borrowing* service (where it does not

constitute a *durable medium*) where the *website conditions* are satisfied.

9.2.2 G (1) Where a *retail client* has provided express prior consent for a *firm* to use any yield earned in further *qualifying cryptoasset lending*, as opposed to yield being transferred or allocated to the *retail client* immediately, the *firm* is not required to provide the information in *CRYPTO* 9.2.1R again in relation to the use of yield in further *qualifying cryptoasset lending*.

(2) This is provided the use of any yield in further *qualifying cryptoasset lending* is on terms that are the same as, or substantially similar to, the original *qualifying cryptoasset lending* service.

(3) A *firm* should nonetheless consider whether it would be in the best interests of the *retail client* for information about any further *qualifying cryptoasset lending* to be provided even where this is not required.

9.2.3 R A *firm* must regularly – and at least once every 3 *months* – review the information provided under *CRYPTO* 9.2.1R(1). If necessary, the *firm* must update the information as soon as possible, to ensure it remains accurate and up to date.

9.2.4 R A *firm* must notify a *retail client* in good time about any material change to the information provided under *CRYPTO* 9.2.1R(1) relevant to the *qualifying cryptoasset lending or borrowing* service that the *firm* is providing to that *retail client*.

Content of the information

9.2.5 R The information in *CRYPTO* 9.2.1R(1) must include:

(1) information about the *qualifying cryptoasset lending or borrowing* service to be provided to the *retail client*;

(2) information about the *qualifying cryptoassets* that will be provided pursuant to the *qualifying cryptoasset lending or borrowing* service;

(3) information about the transfer and return of the *qualifying cryptoassets* or equivalent *qualifying cryptoassets* provided or received as part of the *qualifying cryptoasset lending or borrowing* service and any yield earned or *qualifying cryptoasset borrowing collateral* provided;

(4) information about the *retail client's* access to their *qualifying cryptoassets* or equivalent *qualifying cryptoassets* and access to any yield earned;

(5) information about any restrictions, minimum thresholds and eligibility requirements for the *qualifying cryptoasset lending or borrowing* service;

(6) information about risks;

(7) any other information material to a *retail client's* understanding of the *qualifying cryptoasset lending or borrowing* service; and

(8) when the information was last updated.

Information about the qualifying cryptoasset lending or borrowing service

9.2.6 R Information about the *qualifying cryptoasset lending or borrowing* service to be performed for the *retail client* must include:

(1) the *qualifying cryptoasset lending or borrowing* service to be performed;

(2) how yield is generated for *qualifying cryptoasset lending*, if applicable; and

(3) the loan levels and limits modelled pursuant to *CRYPTO* 9.8.1R.

Information about the qualifying cryptoassets

9.2.7 G (1) A *firm* should provide further information, where appropriate, on the type, nature and uses of the relevant *qualifying cryptoassets*, and their blockchains, associated with the *qualifying cryptoasset lending or borrowing* service provided. This could include providing links to *QCDDs* published in accordance with *CRYPTO* 3.

(2) *Firms* are reminded of the requirements, where applicable, in *CRYPTO* 5.3.7R to make available:

(a) the *QCDD* and *supplementary disclosure document* for the *qualifying cryptoassets*; and/or

(b) the *stablecoin QCDD* for the *UK qualifying stablecoin*,

in respect of which a *firm* deals or arranges deals.

(3) In this chapter, including in relation to (1), a reference to a 'type' of *qualifying cryptoasset*:

(a) refers to a *qualifying cryptoasset* on a specific network that uses distributed ledger technology (eg, blockchain); and

(b) may include reference to the *digital token identifier*, such as the Digital Token Identifier system outlined in ISO standard 24165.

Information about transfer and return

9.2.8 G (1) The information about the transfer and return of the *qualifying cryptoassets* or equivalent *qualifying cryptoassets* provided or received as part of the *qualifying cryptoasset lending or borrowing* service, and any yield earned or *qualifying cryptoasset borrowing collateral* provided should include, where applicable:

(a) information about any restrictions, including those not set by the *firm* itself, on the *retail client's* ability to cease the *qualifying cryptoasset lending or borrowing* service being performed for them, and to receive the return of their *qualifying cryptoassets* or equivalent *qualifying cryptoassets*, and any yield earned or *qualifying cryptoasset borrowing collateral* provided; and

(b) information about the amount of time required for the *qualifying cryptoassets* or equivalent *qualifying cryptoassets* provided or received as part of the *qualifying cryptoasset lending or borrowing* service, and any yield earned or *qualifying cryptoasset borrowing collateral* provided, to be returned to the *retail client*, and whether and in what circumstances the amount of time is variable.

(2) In this chapter, including in (1), a reference to an 'equivalent' *qualifying cryptoasset* means the same type of *qualifying cryptoasset*, unless the *retail client* provides express prior consent to receive or return, as the case may be, a *qualifying cryptoasset* on a different network that uses distributed ledger technology (eg, blockchain) to the *qualifying cryptoasset* originally provided or received as part of the *cryptoasset lending or borrowing* service.

Information about the retail client's access to their qualifying cryptoassets or equivalent qualifying cryptoassets and yield

9.2.9 G The information about the *retail client's* access to their *qualifying cryptoassets* or equivalent *qualifying cryptoassets* and/or access to any yield earned should include, where applicable:

(1) what access the *retail client* will have to their *qualifying cryptoassets* or equivalent *qualifying cryptoassets* while those *qualifying cryptoassets* are engaged in the *qualifying cryptoasset lending* service, including whether the *qualifying cryptoassets* can be transferred or sold at the *retail client's* direction;

(2) whether any yield is safeguarded for the *retail client*, paid directly to the retail client, re-invested or re-used for the benefit of the *retail client*, or used or applied by the *firm* or another *person*; and

(3) the implications of any transfer of ownership of the *retail client's qualifying cryptoassets* and/or any yield earned, including the implications in the event of the insolvency of the *firm* or any other relevant *person* who is safeguarding any *qualifying cryptoassets* and/or yield earned on behalf of the *retail client*.

Information about risks

9.2.10 R The information about risks must include:

(1) an explanation of the types of risks that may be relevant in relation to *qualifying cryptoasset lending or borrowing*, including that the *retail client* may lose some or all of their *qualifying cryptoassets*, any yield earned, or *qualifying cryptoasset borrowing collateral* provided in the event of operational disruption;

(2) in the case of *qualifying cryptoasset lending*, if applicable, an explanation as to how the *firm* mitigates counterparty risk arising from its yield-generating activities using *qualifying cryptoassets* provided by *retail clients* to be used in the *qualifying cryptoasset lending* services; and

(3) an explanation of any other risks of which a *retail client* ought to be aware.

9.2.11 G When considering its approach to the preparation and provision of information in this section, a *firm* should take into account obligations in the *Handbook* that may be relevant, including but not limited to the *Consumer Duty*, and obligations elsewhere in *PRIN* and in *COBS.*

9.3 Key terms of agreement and express prior consent requirement

The express prior consent requirement

9.3.1 R (1) A *firm* must provide a *retail client* with the key terms of agreement relating to its *qualifying cryptoasset lending or borrowing* services.

(2) A *firm* must obtain the *retail client's* express prior consent in relation to those key terms of agreement:

(a) each time that *retail client* instructs the *firm* to provide the *qualifying cryptoasset lending or borrowing* services; and

(b) before one of the following, whichever is the earlier:

(i) the *retail client* is bound by any agreement relating to the *qualifying cryptoasset lending or borrowing* services; or

(ii) the provision of those services.

(3) A *firm* must provide the key terms of agreement in a *durable medium* or via a website, mobile application or any other digital medium that the *firm* may be using in relation to the provision of its *qualifying cryptoasset lending or borrowing* service (where it does not constitute a *durable medium*) where the *website conditions* are satisfied.

(4) The *firm* must keep a record of the *retail client's* express prior consent that is capable of being produced or reproduced upon the *FCA's* request.

(5) The key terms in respect of which a *retail client* must provide express prior consent must include the terms set out in *CRYPTO* 9.3.3R.

9.3.2 G (1) Where a *retail client* has provided express prior consent for a *firm* to use any yield earned in further *qualifying cryptoasset lending*, as opposed to yield being transferred or allocated to the *retail client* immediately, the *firm* is not required to obtain the *retail client's* express prior consent again in relation to the use of yield in further *qualifying cryptoasset lending*.

(2) This is provided the use of any yield in further *qualifying cryptoasset lending* is on terms that are the same as, or substantially similar to, the original *qualifying cryptoasset lending* service.

Key terms

9.3.3 R The terms in respect of which a *firm* must obtain a *retail client's* express prior consent include, if applicable:

(1) the type and quantity of the *qualifying cryptoassets* the *firm* will provide or receive as part of the *qualifying cryptoasset lending or borrowing* service for the *retail client*;

(2) how long the *qualifying cryptoassets* will be engaged in the *qualifying cryptoasset lending or borrowing* service;

(3) the value of the *qualifying cryptoassets* the *firm* will provide or receive as part of the *qualifying cryptoasset lending or borrowing* service;

(4) the duration of the loan of *qualifying cryptoassets* to or from the *retail client* and whether that duration is fixed or flexible;

(5) the total and component parts of one-off and ongoing charges, fees and commission, including exit fees, to be paid by the *retail client* to the *firm* or any third parties for the *qualifying cryptoasset lending or borrowing* service;

(6) in relation to *qualifying cryptoasset lending* only, the treatment of yield that may be earned and transferred to the *retail client*;

(7) in relation to *qualifying cryptoasset borrowing* only:

(a) the amount of *qualifying cryptoasset borrowing collateral* that must be provided by the *retail client*;

(b) the amount of interest payable by the *retail client*, if any;

(c) the *firm's* ability to supplement the *retail client's qualifying cryptoasset borrowing collateral* on the *retail client's* behalf pursuant to *CRYPTO* 9.6.4R;

(d) the *firm's* ability to realise the *qualifying cryptoasset borrowing collateral*; and

(e) the loan limits set by the *firm* pursuant to *CRYPTO* 9.8.1R(1) or by the *retail client* pursuant to *CRYPTO* 9.8.5R;

(8) any restrictions set by the *firm* on a *retail client's* ability to access their *qualifying cryptoassets* or equivalent *qualifying cryptoassets* provided or received as part of the *qualifying cryptoasset lending or borrowing* service;

(9) the *retail client's* ability to terminate the *qualifying cryptoasset lending or borrowing* service and receive a return of their *qualifying cryptoassets* or equivalent *qualifying cryptoassets* and any yield earned or *qualifying cryptoasset borrowing collateral* provided, including whether any financial penalties may be incurred by the *retail client*;

(10) the amount of time the *firm* requires to restore the *retail client's* access to their *qualifying cryptoassets* or equivalent *qualifying cryptoassets* and any accrued yield and/or *qualifying cryptoasset borrowing collateral* provided, following receipt of a request to terminate the *qualifying cryptoasset lending or borrowing* service;

(11) whether ownership of the *retail client's qualifying cryptoassets* transfers from the *retail client* to the *firm* or any other *person* as part of the *qualifying cryptoasset lending or borrowing* service;

(12) whether the *retail client's qualifying cryptoassets* engaged in the *qualifying cryptoasset lending or borrowing* service and/or any yield earned are being safeguarded on trust by the *firm* or any other person on behalf of the *retail client*; and

(13) whether any *qualifying cryptoasset borrowing collateral* provided by the *retail client* is safeguarded on trust by the *firm* or any other person on behalf of the *retail client*.

9.3.4 G (1) In relation to *CRYPTO* 9.3.3R(3), a *firm* should take all reasonable steps to obtain the most recent valuation for the *qualifying cryptoassets* that will be engaged in the *qualifying cryptoasset lending or borrowing* service.

(2) This value referred to in (1) should be presented in GBP.

9.3.5 G In relation to *CRYPTO* 9.3.3R(5), a *firm* should:

(1) present one-off charges and fees for the *qualifying cryptoasset lending or borrowing* service as both a monetary value in GBP and as a percentage of the total value of *qualifying cryptoassets* engaged in the *qualifying cryptoasset lending or borrowing* service;

(2) in presenting the information in (1), take all reasonable steps to obtain the most recent valuation of those *qualifying cryptoassets* and express the monetary value of the charge or fee;

(3) set out what fees and charges may be payable to third parties, including gas fees and settlement fees;

(4) make clear which charges originate from the blockchain, such as gas fees, and which charges are levied by the *firm*; and

(5) explain how any fees, charges or interest rates (if applicable) may vary through the duration of the *qualifying cryptoasset lending or borrowing* service and how such variations will be communicated to the *retail client*.

9.3.6 R In relation to *CRYPTO* 9.3.3R(6), the terms must include:

(1) what the applicable rate of yield is and how it is determined;

(2) in the case of a variable rate, how that rate is calculated and how any variations will be communicated to the *retail client*;

(3) in what *qualifying cryptoasset* or currency the yield will be paid or provided to the *retail client*;

(4) the frequency with which yield may be earned and paid or provided to the *retail client* and, if the frequency is variable, on what basis it will vary;

(5) what commission the *firm* will take, presented as a percentage of the total yield earned; and

(6) whether:

(a) any yield earned is transferred to the *retail client* or safeguarded for the *retail client*;

(b) the *firm* is permitted to use or re-invest the yield;

(c) the yield is used in further *qualifying cryptoasset lending or borrowing* or other activities and/or what investment activities the *firm* uses to generate further yield; and

(d) the *retail client* retains a claim on that yield on insolvency of the *firm* or otherwise.

9.3.7 R In relation to *CRYPTO* 9.3.3R(7), the terms must include:

(1) the market value of the initial *qualifying cryptoasset borrowing collateral* provided by the *retail client*; and

(2) the maximum additional *qualifying cryptoasset borrowing collateral* expressed in terms of its market value, subject to *CRYPTO* 9.6.4R to *CRYPTO* 9.6.6R.

9.3.8 G When setting out the market value of the *qualifying cryptoasset borrowing collateral* as required by *CRYPTO* 9.3.7R, a *firm* should take all reasonable steps to obtain the most recent valuation, presented in GBP.

Material changes

9.3.9 R A *firm* must notify a *retail client* in good time about any material change to the key terms of agreement provided under *CRYPTO* 9.3.1R(1) relevant to the *qualifying cryptoasset lending or borrowing* service that the *firm* is providing to that *retail client*.

9.3.10 G When considering its approach to preparing and providing key terms of agreement and obtaining express prior consent in respect thereof, as well as its approach to notifications about material changes to key terms, a *firm* should take into account obligations in the *Handbook* that may be relevant. These may include, but are not limited to the *Consumer Duty* and obligations elsewhere in *PRIN* and in *COBS*, as well as obligations in consumer rights law and any associated and applicable guidance.

9.4 Record keeping requirements

9.4.1 R The provisions in this section apply to an *authorised cryptoasset firm* when providing a *qualifying cryptoasset lending or borrowing* service to any *client* who is not an *overseas client*.

9.4.2 R (1) A *firm* must maintain records of the following:

(a) the amount of *qualifying cryptoassets* provided or received in a *qualifying cryptoasset lending or borrowing* service for each *client* and on which blockchain, per day;

(b) whether the *qualifying cryptoassets* are safeguarded for the *client* and, if so, by whom;

(c) the total amount of yield earned in relation to the *qualifying cryptoasset lending* service performed for each *client*, per day;

(d) for each *client* to whom the *firm* provides any *qualifying cryptoasset lending* service:

(i) a list of the types of *qualifying cryptoassets* provided in a *qualifying cryptoasset lending* arrangement by the *client* to the *firm*;

(ii) the quantity of each *qualifying cryptoasset* provided in a *qualifying cryptoasset lending* arrangement by the *client* to the *firm*; and

(iii) the relevant virtual address for each *qualifying cryptoasset* provided in a *qualifying cryptoasset lending* arrangement by the *client* to the *firm*;

(e) total fees, charges, interest or commission charged to each *client* per day;

(f) where applicable, the key terms of agreement provided to each *client* and each *client's* express prior consent provided in relation thereto, including the date, time and amount of *qualifying cryptoassets* provided or received pursuant to the *qualifying cryptoasset lending or borrowing* service;

(g) all notifications provided to the *client* pursuant to *CRYPTO* 9.2.4R;

(h) all notifications provided to the *client* pursuant to *CRYPTO* 9.3.9R;

(i) all requests from *clients* to terminate the *qualifying cryptoasset lending or borrowing* service or for the *client's qualifying cryptoassets* to be returned, including the date, time and amount of *qualifying cryptoassets* requested to be returned; and

(j) the total amount of *qualifying cryptoassets* provided or received in the *qualifying cryptoasset lending or borrowing* service lost per day due to operational disruptions.

(2) Subject to (3), all records in (1) must be retained for a period of 5 years from the point at which the record is generated.

(3) The records specified in (1)(f) to (h) must be retained for a period of at least 5 years from the point at which the record is generated or for the duration of the relationship with the *client*, whichever is longer.

9.5 Proprietary token restriction

9.5.1 R (1) A *firm* must not use a *proprietary token* in connection with its *qualifying cryptoasset lending or borrowing* service.

(2) For the purposes of (1), this includes:

(a) accepting *proprietary tokens* from *retail clients* as part of *qualifying cryptoasset lending or borrowing*;

(b) providing *proprietary tokens* to *retail clients* as part of *qualifying cryptoasset borrowing*;

(c) accepting *proprietary tokens* from *retail clients* as *collateral* for *qualifying cryptoasset borrowing*;

(d) paying yield to *retail clients* in a *proprietary token*; and

(e) offering more favourable yield or interest rates for *qualifying cryptoasset lending or borrowing* for *retail clients* who hold or own *proprietary tokens*.

9.6 Qualifying cryptoasset borrowing collateral

Provision of qualifying cryptoasset borrowing collateral

9.6.1 R This section applies to a *firm* when it provides a *qualifying cryptoasset borrowing* service to *retail clients*.

9.6.2 R (1) A *firm* providing a *qualifying cryptoasset borrowing* service to a *retail client* must require *qualifying cryptoasset borrowing collateral* to be provided by the *retail client* to the *firm* before the provision of the *qualifying cryptoasset borrowing* service.

(2) The amount of *qualifying cryptoasset borrowing collateral* to be provided by the *retail client* under (1) must have a market value that exceeds the market value of the *qualifying cryptoassets* provided to the *retail client* as part of the *qualifying cryptoasset borrowing* service.

9.6.3 G *CRYPTO* 9.6.2R(1) does not require the *firm* itself to receive the *qualifying cryptoasset borrowing collateral* from the *retail client*. The *firm* may arrange for another *person* to safeguard the *qualifying cryptoasset borrowing collateral* for the *retail client*, in accordance with the conditions set out in *CRYPTO* 9.6.8R.

Additional qualifying cryptoasset borrowing collateral

9.6.4 R (1) Subject to (3) and (4) and *CRYPTO* 9.6.5R to *CRYPTO* 9.6.6R, a *firm* may provide for *retail clients* to supplement their initial *qualifying cryptoasset borrowing collateral*.

(2) In relation to (1), a *firm* may:

(a) allow for *retail clients* to supplement their initial *qualifying cryptoasset borrowing collateral* themselves; and/or

(b) provide a facility in terms of which the *firm* may supplement the initial *qualifying cryptoasset borrowing collateral* on the *retail client's* behalf.

(3) Where a *firm* provides the facility in (2)(b) to supplement the initial *qualifying cryptoasset borrowing collateral* on the *retail client's* behalf, the *firm* must obtain the *retail client's* express prior consent.

(4) Where a *retail client* has provided express prior consent per (3), the *firm* may only exercise this right in relation to assets or currency that the *retail client* has expressly made available for that purpose.

9.6.5 R (1) Where a *retail client* has provided express prior consent for the *firm* to supplement its *qualifying cryptoasset borrowing collateral* on that *retail client's* behalf pursuant to *CRYPTO* 9.6.4R(2)(b), the total additional assets (which may include *qualifying cryptoassets*) or currency that may be applied to the *retail client's* initial *qualifying cryptoasset borrowing collateral*, whether in one or more applications, must not exceed 50% of the market value of the initial *qualifying cryptoasset borrowing collateral* at the commencement of the *qualifying cryptoasset borrowing* service.

(2) For the purposes of (1), any fees, charges or interest payable by the *retail client* in respect of the *qualifying cryptoasset borrowing* must be deducted from the maximum additional *qualifying cryptoasset borrowing collateral* amount.

9.6.6 R (1) Prior to the commencement of a *qualifying cryptoasset borrowing* service, a *firm* must provide a *retail client* with the option to set a limit on the amount by which the *firm* may supplement the initial *qualifying cryptoasset borrowing collateral* on the *retail client's* behalf pursuant to *CRYPTO* 9.6.4R(2)(b).

(2) The limit chosen by the *retail client* may not be higher than the maximum additional *qualifying cryptoasset borrowing collateral* amount prescribed under *CRYPTO* 9.6.5R.

9.6.7 G (1) *CRYPTO* 9.6.5R and *CRYPTO* 9.6.6R apply only in relation to the supplementing of a *retail client's qualifying cryptoasset borrowing*

collateral by the *firm* on the *retail client's* behalf pursuant to *CRYPTO* 9.6.4R(2)(b).

(2) Nothing in this section is intended to prevent a *retail client* from supplementing their *qualifying cryptoasset borrowing collateral* themselves, including by providing additional assets or currency directly, during the *qualifying cryptoasset borrowing* service.

Restriction on re-use of qualifying cryptoasset borrowing collateral

9.6.8 R (1) Where the *qualifying cryptoasset borrowing collateral* provided by a *retail client* pursuant to *CRYPTO* 9.6.2R(1) is a *qualifying cryptoasset* or *relevant specified investment cryptoasset*, a *firm* must ensure the outcome in either (a) or (b), and must also comply with (c):

(a) Provided the *firm* has *Part 4A permission* to carry on *safeguarding cryptoassets*, the *firm* structures the collateral arrangements so that it is itself carrying on the *regulated activity* of *safeguarding cryptoassets* in relation to the *qualifying cryptoasset borrowing collateral*.

(b) Provided the *firm* has *Part 4A permission* to carry on *arranging cryptoasset safeguarding*, the *firm* structures the collateral arrangements so that it carries on the *regulated activity* of *arranging cryptoasset safeguarding* in relation to the *qualifying cryptoasset borrowing collateral*, with the effect that an *authorised person* with *permission* to carry on the *regulated activity* of *safeguarding cryptoassets* is carrying on that *regulated activity* for the *firm's retail client* in relation to the *qualifying cryptoasset borrowing collateral*.

(c) The *firm* must ensure that any collateral arrangements in the course of either (a) or (b) do not result in the *firm* or any other *person* obtaining full ownership of the *qualifying cryptoasset borrowing collateral* other than where the *retail client* has provided express prior consent to a transfer of full ownership in order to discharge the *retail client's* indebtedness to the *firm* in relation to the *qualifying cryptoasset borrowing* service in accordance with *CASS* 17.3.10R.

(2) Where the *qualifying cryptoasset borrowing collateral* provided by the *retail client* pursuant to *CRYPTO* 9.6.2R(1) is a *security* or *contractually based investment*, a *firm* must ensure the outcome in either (a) or (b), and must also comply with (c):

(a) Provided the *firm* has *Part 4A permission* to carry on *safeguarding and administering investments*, the *firm* structures the collateral arrangements so that it is itself carrying on the *regulated activity* of *safeguarding and*

administering investments in relation to the *qualifying cryptoasset borrowing collateral*.

(b) Provided the *firm* has *Part 4A permission* to carry on *arranging safeguarding and administration of assets*, the *firm* structures the collateral arrangements so that it arranges for one or more other *persons* to safeguard the *qualifying cryptoasset borrowing collateral*, with the effect that an *authorised person* with *permission* to carry on the *regulated activity* of *safeguarding and administering investments* is carrying on that *regulated activity* for the *firm's retail client* in relation to the *qualifying cryptoasset borrowing collateral*.

(c) The *firm* must ensure that any collateral arrangements in the course of either (a) or (b) do not result in the *firm* or any other *person* obtaining full ownership of the *qualifying cryptoasset borrowing collateral* other than where the *retail client* has provided express prior consent to a transfer of full ownership in order to discharge the *retail client's* indebtedness to the *firm* in relation to the *qualifying cryptoasset borrowing* service.

(3) Where the *qualifying cryptoasset borrowing collateral* is *money*, the *firm* must ensure that the collateral arrangements do not result in the *firm* or any other *person* obtaining full ownership of the *qualifying cryptoasset borrowing collateral* other than where the *retail client* has provided express prior consent to a transfer of full ownership in order to discharge the *retail client's* indebtedness to the *firm* in relation to the *qualifying cryptoasset borrowing* service.

9.6.9 G (1) A consequence of *CRYPTO* 9.6.8R(1) is that the *retail client* has the benefit of the protections of the *cryptoasset safeguarding rules* in *CASS* 17 in relation to any *qualifying cryptoasset borrowing collateral* which is a *qualifying cryptoasset* or *specified investment cryptoasset*.

(2) The *rules* at *CASS* 17.3.4R(4) and *CASS* 17.3.6R(6) restrict how that *qualifying cryptoasset borrowing collateral* may be used.

(3) A consequence of *CRYPTO* 9.6.8R(2) is that the *retail client* has the benefit of the protections of the *custody rules* in *CASS* 6 in relation to any *qualifying cryptoasset borrowing collateral* which is a *security* or *contractually based investment*.

9.6.10 G (1) *Firms* should note that the requirements on *qualifying cryptoasset borrowing collateral* in this section, as well as in *CASS* 17, limit how *qualifying cryptoasset borrowing collateral* may be used.

(2) However, the *FCA* considers that it should still be possible for a *firm* to provide a *qualifying cryptoasset staking* service for a *qualifying*

cryptoasset held as *qualifying cryptoasset borrowing collateral* provided:

(a) the *firm* provides the *qualifying cryptoasset staking* service in compliance with the staking rules in *CRYPTO* 10;

(b) neither the *firm* nor any other *person* obtains full ownership of the *qualifying cryptoasset borrowing collateral*, as set out in *CRYPTO* 9.6.8R(1); and

(c) the *qualifying cryptoasset borrowing collateral* is safeguarded as *client cryptoassets* in accordance with *CASS* 17.3.3R.

(3) This means that a *firm* that wishes to provide a *qualifying cryptoasset staking* service using a *qualifying cryptoasset* held as *qualifying cryptoasset borrowing collateral* will need to consider carefully the way in which that *qualifying cryptoasset staking* may be performed and the technical features of that *qualifying cryptoasset staking* to ensure the *firm's* compliance with its obligations is not undermined.

9.7 Negative balance protection

9.7.1 R The liability of a *retail client* for any *qualifying cryptoasset borrowing* is limited to the market value of any *qualifying cryptoasset borrowing collateral* (including any additional *qualifying cryptoasset borrowing collateral* provided pursuant to *CRYPTO* 9.6.4R) provided by the *retail client*.

9.7.2 G *CRYPTO* 9.7.1R means that a *retail client* cannot lose more than the *qualifying cryptoasset borrowing collateral* (including any additional *qualifying cryptoasset borrowing collateral* provided pursuant to *CRYPTO* 9.6.4R) specifically dedicated for the purpose of engaging in *qualifying cryptoasset borrowing*.

9.8 Loan levels and limits

Modelling of loan parameters

9.8.1 R (1) A *firm* must, prior to offering a *qualifying cryptoasset borrowing* service to a *retail client*, model and set limits for:

(a) the loan-to-value ratio;

(b) the margin call level; and

(c) the liquidation level.

(2) The *firm* must base the limits in (1) on modelling of previous price performance and volatility of the *qualifying cryptoasset borrowing collateral* and *qualifying cryptoassets* provided to the *retail client* as part of the *qualifying cryptoasset borrowing* service. On this basis,

margin calls and liquidation should not be expected to occur within the first 6 *months* following the commencement of the *qualifying cryptoasset borrowing* service.

9.8.2 G In *CRYPTO* 9.8.1R(1)(c), 'liquidation level' refers to the loan-to-value ratio at which the *firm* is entitled to realise some or all of the *retail client's qualifying cryptoasset borrowing collateral* to discharge the *retail client's* indebtedness to the *firm* in relation to the *qualifying cryptoasset borrowing* service.

9.8.3 G *Firms* should note that the risk of liquidation will likely increase the higher the loan-to-value ratio is set, even if all other factors remain constant.

9.8.4 R Modelling and limit-setting should be conducted without factoring in any potential additional *qualifying cryptoasset borrowing collateral* that may supplement the initial *qualifying cryptoasset borrowing collateral* provided by the *retail client*.

9.8.5 R (1) A *firm* must, prior to entering into an agreement relating to its *qualifying cryptoasset borrowing* service with a *retail client*, provide the *retail client* with the option to set their own limits for:

(a) the loan-to-value ratio;

(b) the margin call level; and

(c) the liquidation level (including both full and partial liquidation levels).

(2) The limit(s) set by the *retail client* may not be higher than the levels modelled by the *firm* under *CRYPTO* 9.8.1R.

9.9 Client reporting requirements

9.9.1 R This section applies to a *firm* when providing a *qualifying cryptoasset lending or borrowing* service to a *client*.

Reporting transactions

9.9.2 R (1) A *firm* must provide a report to each *client* on the execution of each *qualifying cryptoasset lending or borrowing* transaction that relates to them.

(2) This report must be provided promptly and no later than 23:59:59 UTC on the day on which the order was executed or on which the information was received by the *firm*.

9.9.3 R A *firm* does not need to provide a report in accordance with *CRYPTO* 9.9.2R where a *client* has agreed in writing they do not want to receive it on this basis.

9.9.4 G Where a *firm* and its *client* agree to proceed in accordance with *CRYPTO* 9.9.3R, the *firm* may provide reports to that *client* on an aggregated basis on terms to be agreed with that *client*.

9.9.5 G For the purposes of *CRYPTO* 9.9.2R(1), a *qualifying cryptoasset lending or borrowing* transaction includes all transactions between the *firm* and its *client* in the course of a *qualifying cryptoasset lending or borrowing* arrangement.

9.9.6 R A *firm* must provide the information required in this section in a *durable medium* or via a website, mobile application or any other digital medium that the *firm* may be using in relation to the provision of its *qualifying cryptoasset lending or borrowing* service (where it does not constitute a *durable medium*) where the *website conditions* are satisfied.

Cancellations

9.9.7 R (1) Where a *qualifying cryptoasset lending or borrowing* transaction has been cancelled, a *firm* must provide the *client* with confirmation of, and a reason for, the cancellation.

(2) The information in (1) must be provided promptly and no later than 23:59:59 UTC on the day on which the order was cancelled.

Client requests for information

9.9.8 R A *client* may request, at any time, that a *firm* provide them with the information in *CRYPTO* 9.9.9R, in relation to that *client*:

(1) for all *qualifying cryptoasset lending or borrowing* transactions (including cancellations);

(2) for the period of 3 years preceding the request; and

(3) in a medium compliant with *CRYPTO* 9.9.6R,

irrespective of whether they agree with the *firm* not to receive a report in accordance with *CRYPTO* 9.9.2R.

Content of client reports

9.9.9 R The report provided by a *firm* under *CRYPTO* 9.9.2R(1) must include all information identified in column (2) of *CRYPTO* 9 Annex 1.

Periodic reporting

9.9.10 R (1) A *firm* which provides *qualifying cryptoasset lending or borrowing* services to a *client* must provide the *client* with a *periodic statement* unless:

(a) such a statement is provided by another *person*; or

(b) all of the conditions in (2) are satisfied.

(2) The conditions referred to (1)(b) are that:

(a) the *firm* provides the *client* with access to an online system, application or digital medium which meets the requirements in *CRYPTO* 9.9.6R;

(b) the system in (a) provides the *client* with easy access to up-to-date valuations of the information identified in column (3) of the table in *CRYPTO* 9 Annex 1; and

(c) the *firm* has evidence that the *client* has accessed the online system in (a) at least once during the previous quarter.

(3) The *periodic statement* must include the information identified in column (3) of *CRYPTO* 9 Annex 1.

9.9.11 R The *periodic statement* must be provided once every 6 *months*, except in the following cases:

(1) if the *retail client* so requests, the *periodic statement* must be provided every 3 *months*; or

(2) if the *client* has agreed in writing they do not want to receive the *periodic statement* on this basis and elects to solely receive information about a *qualifying cryptoasset lending or borrowing* arrangement on a transaction-by-transaction basis, the *periodic statement* must be provided at least once every 12 *months*.

9.9.12 R A *firm* must inform a *retail client* that they have the right to request the provision of a *periodic statement* every 3 *months*.

9.10 Obligations in COBS

9.10.1 G A *firm* may satisfy its obligations in this chapter and any other applicable provisions in *COBS* by means of a single set of systems, controls, policies, procedures, communications or contractual arrangements, provided that those arrangements, taken as a whole, meet the requirements of each applicable provision in this chapter and *COBS*.

9.10.2 G The purpose of this section is to avoid unnecessary duplication of systems, controls and client interactions where a *firm* is subject to overlapping requirements under this chapter and other *COBS* provisions.

9 Annex 1 Information to be provided to qualifying cryptoasset lending or borrowing clients

9 Annex 1 R

	(1) **Data field**	(2) **Trade confirmation information**	(3) **Periodic report information**
(1)	The name of the *firm*	N	Y
(2)	The name or other designation of the *client's* account	N	Y
(3)	The amount of *qualifying cryptoassets* provided by the *firm* to the *client* in the *qualifying cryptoasset lending or borrowing* transaction	Y	Y
(4)	The total amount of *qualifying cryptoassets* provided to, or received by, the *client* in a *qualifying cryptoasset lending or borrowing* arrangement	N	Y
(5)	The type of each *qualifying cryptoasset* provided in a *qualifying cryptoasset lending* transaction or arrangement by the *client* to the *firm*	Y	Y
(6)	The total amount of yield owed to the *client* by the *firm* in relation to the *qualifying cryptoasset lending* arrangement	N	Y
(7)	The total amount of yield paid to the *client* by the *firm* in relation to the *qualifying*	N	Y

	cryptoasset lending arrangement		
(8)	The fees, charges, interest or commission (expressed in GBP) which have been charged to the *client* for the *qualifying cryptoasset lending or borrowing* transaction	Y	N
(9)	The total fees, charges, interest or commission (expressed in GBP) charged to the *client* for each *qualifying cryptoasset lending or borrowing* arrangement	N	Y
(10)	The total amount of *qualifying cryptoassets* provided or received in the *qualifying cryptoasset lending or borrowing* arrangement lost per day due to operational disruptions	N	Y
(11)	The *qualifying cryptoasset borrowing collateral* provided by the *client* for each *qualifying cryptoasset borrowing* arrangement	N	Y
(12)	The value of the *qualifying cryptoasset borrowing collateral* provided by the *client* for each *qualifying cryptoasset borrowing* arrangement in GBP	Y	Y
(13)	Whether the *qualifying cryptoassets* provided by the *client* for *qualifying cryptoasset borrowing collateral*	Y	Y

	are safeguarded by the *firm* or another party		
(14)	The identity of any third party safeguarding the *qualifying cryptoasset borrowing collateral* provided by the *client*	Y	Y
(15)	The outstanding balance owed by the *client* to the *firm* in a *qualifying cryptoasset borrowing* arrangement	N	Y
(16)	Details of the remainder of any loan period of a *qualifying cryptoasset borrowing* arrangement	N	Y

10 Qualifying cryptoasset staking

10.1 Application

Who? What?

10.1.1 R (1) Except as provided for in (2), this chapter applies to an *authorised cryptoasset firm* when *arranging qualifying cryptoasset staking* for a *retail client*.

(2) For the purposes of *CRYPTO* 10.5, the record keeping requirements apply to an *authorised cryptoasset firm* when *arranging qualifying cryptoasset staking* for any *client*.

10.1.2 G In this chapter, 'auto-staking' means a *qualifying cryptoasset staking* service where:

(1) the *retail client* has designated a type of *qualifying cryptoasset* to be used in a *qualifying cryptoasset staking* service;

(2) the future holdings of the type of *qualifying cryptoasset* designated by the *retail client* are to be used in *qualifying cryptoasset staking*; and

(3) the *firm* is *safeguarding cryptoassets* or *arranging cryptoasset safeguarding* of the future holdings of *qualifying cryptoassets* designated by the *retail client*.

10.1.3 G In this chapter, unless indicated otherwise or the context clearly indicates otherwise, references to a '*qualifying cryptoasset staking* service' should be read as including references to auto-staking.

10.1.4 G For the purposes of *CRYPTO* 10.2.4R, *CRYPTO* 10.3.8R, *CRYPTO* 10.4.1R and *CRYPTO* 10.5.3R, references to a '*retail client*' or '*client*' (as the case may be) who the *firm* is required to notify need only include a *retail client* or *client* where known to the *firm*.

10.2 Information requirement

10.2.1 R (1) A *firm* must provide a *retail client* with information about the *firm* and its *qualifying cryptoasset staking* service.

(2) The information in (1) must be provided to a *retail client*:

(a) each time that *retail client* instructs the *firm* to provide the *qualifying cryptoasset staking* service; and

(b) before one of the following, whichever is the earlier:

(i) a *retail client* is bound by any agreement relating to *qualifying cryptoasset staking*; or

(ii) the provision of those services.

(3) A *firm* must provide the information in (1) in a *durable medium* or via a website, mobile application or any other digital medium that the *firm* may be using in relation to the provision of its *qualifying cryptoasset staking* service (where it does not constitute a *durable medium*) where the *website conditions* are satisfied.

10.2.2 G (1) Where a *retail client* has provided express prior consent for the *firm* to use any rewards earned in further *qualifying cryptoasset staking*, as opposed to rewards being transferred or allocated to the *retail client* immediately, the *firm* is not required to provide the information in *CRYPTO* 10.2.1R again in relation to the use of rewards in further *qualifying cryptoasset staking*.

(2) This is provided the use of any rewards in further *qualifying cryptoasset staking* is on terms that are the same as, or substantially similar to, the original *qualifying cryptoasset staking* service.

(3) A *firm* should nonetheless consider whether it would be in the best interests of the *retail client* for it to provide information about any further *qualifying cryptoasset staking* even where this is not required.

10.2.3 R A *firm* must regularly – and at least once every 3 *months* – review the information provided under *CRYPTO* 10.2.1R(1). If necessary, the *firm* must

update the information as soon as possible, to ensure it remains accurate and up to date.

10.2.4 R A *firm* must notify a *retail client* in good time about any material change to the information provided under *CRYPTO* 10.2.1R(1) relevant to the *qualifying cryptoasset staking* service that the *firm* is providing to that *retail client*.

Content of the information

10.2.5 R The information in *CRYPTO* 10.2.1R(1) must include:

(1) information about the *qualifying cryptoasset staking* service to be provided to the *retail client*;

(2) information about the *qualifying cryptoassets* that will be used in the *qualifying cryptoasset staking* service;

(3) information about the transfer and return of *qualifying cryptoassets* used in the *qualifying cryptoasset staking* service and any rewards earned;

(4) information about the *retail client's* access to their *qualifying cryptoassets* and access to rewards earned;

(5) information about risks;

(6) any other information material to a *retail client's* understanding of the *qualifying cryptoasset staking* service; and

(7) when the information was last updated.

Information about the qualifying cryptoasset staking service

10.2.6 G Information about the *qualifying cryptoasset staking* service to be performed for the *retail client* should include:

(1) a description of the *qualifying cryptoasset staking* service, including whether the *qualifying cryptoasset staking* will be performed by the *firm* itself or by another *person* or *persons*; and

(2) where a *qualifying cryptoasset staking* service involves auto-staking, an explanation that the *firm* will use a *retail client's* future holdings of one or more of the types of *qualifying cryptoassets* that the *retail client* has designated for that purpose in *qualifying cryptoasset staking*.

Information about the qualifying cryptoassets

10.2.7 G (1) The information about the *retail client's qualifying cryptoassets* to be used in the *qualifying cryptoasset staking* service should include, where applicable:

(a) that the *retail client* may receive a *cryptoasset* as part of the *qualifying cryptoasset staking* service;

(b) that there may be risks associated with any other *cryptoasset* provided as part of the *qualifying cryptoasset staking* service, such as the possibility of a change in value in comparison to the *client's* underlying *qualifying cryptoassets* being used in the *qualifying cryptoasset staking* service;

(c) information on the functions and limitations of any other *cryptoasset* provided as part of the *qualifying cryptoasset staking* service, including whether it can be transferred, sold or used in any other *qualifying cryptoasset staking* service;

(d) the implications for the *retail client* of the transfer to another *person* of any *cryptoasset* provided to the *retail client* as part of the *qualifying cryptoasset staking* service; and

(e) information on how any other *cryptoasset* provided to the *retail client* may be returned to, or exchanged with, the *firm* or another *person* for the *qualifying cryptoasset* being used in the *qualifying cryptoasset staking* service, and any rewards earned (as applicable).

(2) A *firm* should provide further information, where appropriate, on the type, nature and uses of the relevant *qualifying cryptoassets*, and their blockchains, associated with the *qualifying cryptoasset staking* service provided. This could include providing links to *QCDDs* published in accordance with *CRYPTO* 3.

(3) In this chapter, including in (2), a reference to a 'type' of *qualifying cryptoasset*:

(a) refers to a *qualifying cryptoasset* on a specific network that uses distributed ledger technology (eg, blockchain); and

(b) may include reference to the *digital token identifier*, such as the Digital Token Identifier system outlined in ISO standard 24165.

Information about transfer and return

10.2.8 G The information about the transfer and return of *qualifying cryptoassets* used in the *qualifying cryptoasset staking* service and any rewards earned should include, where applicable:

(1) information about any restrictions, including those not set by the *firm* itself, on the *retail client's* ability to cease the *qualifying cryptoasset staking* service being performed for them, and to receive the return of their *qualifying cryptoassets* and any rewards earned, if applicable; and

(2) information about the amount of time required for *qualifying cryptoassets* used in the *qualifying cryptoasset staking* service and any rewards earned, if applicable, to be returned to the *retail client*, and whether and in what circumstances the amount of time is variable.

Information about a retail client's access to their qualifying cryptoassets and rewards

10.2.9 G The information about the *retail client's* access to their *qualifying cryptoassets* and/or access to any rewards earned should include, where applicable:

(1) what access the *retail client* will have to their *qualifying cryptoassets* while those *qualifying cryptoassets* are being used in the *qualifying cryptoasset staking* service, including whether the *qualifying cryptoassets* can be transferred or sold at the *retail client's* direction; and

(2) the implications of any transfer of ownership of the *retail client's qualifying cryptoassets* used in *qualifying cryptoasset staking* and/or any rewards earned, including the implications in the event of the insolvency of the *firm* or any other relevant *person* who is holding any *qualifying cryptoassets* and/or rewards earned on behalf of the *retail client*.

Information about risks

10.2.10 R The information about risks must include, where applicable:

(1) the identity of any *person* or *persons* the *firm* currently uses to perform the *qualifying cryptoasset staking*; and

(2) an explanation of the types of risks that may be relevant in relation to *qualifying cryptoasset staking*, including that the *retail client* may lose some or all of their *qualifying cryptoassets* used in the *qualifying cryptoasset staking* service in the event of operational disruption.

10.2.11 G When considering its approach to the preparation and provision of information in this section, a *firm* should take into account obligations in the Handbook that may be relevant, including but not limited to the *Consumer Duty* and obligations elsewhere in *PRIN* and in *COBS*.

10.3 Key terms of agreement and express prior consent requirement

10.3.1 R (1) A *firm* must provide a *retail client* with the key terms of agreement relating to its *qualifying cryptoasset staking* service.

(2) A *firm* must obtain the *retail client's* express prior consent in relation to the key terms of agreement:

(a) each time that *retail client* instructs the *firm* to provide the *qualifying cryptoasset staking* service; and

(b) before one of the following, whichever is the earlier:

(i) the *retail client* is bound by any agreement relating to *qualifying cryptoasset staking*; or

(ii) the provision of those services.

(3) A *firm* must provide the key terms of agreement in a *durable medium* or via a website, mobile application or any other digital medium that the *firm* may be using in relation to the provision of its *qualifying cryptoasset staking* service (where it does not constitute a *durable medium*) where the *website conditions* are satisfied.

(4) The *firm* must keep a record of the *retail client's* express prior consent that is capable of being produced or reproduced upon the *FCA's* request.

(5) The key terms in respect of which a *retail client* must provide express prior consent must include the terms set out in *CRYPTO* 10.3.3R.

10.3.2 G (1) Where a *retail client* has provided express prior consent for a *firm* to use any rewards earned in further *qualifying cryptoasset staking*, as opposed to rewards being transferred or allocated to the *retail client* immediately, the *firm* is not required to obtain the *retail client's* express prior consent again in relation to the use of rewards in further *qualifying cryptoasset staking*.

(2) This is provided the use of any rewards in further *qualifying cryptoasset staking* is on terms that are the same as, or substantially similar to, the original *qualifying cryptoasset staking* service.

10.3.3 G (1) Where the *qualifying cryptoasset staking* service involves auto-staking, the requirement in *CRYPTO* 10.3.1R applies each time the *retail client* instructs the *firm* to provide an auto-staking service in respect of future holdings of the *retail client's qualifying cryptoassets*.

(2) A *firm* is therefore not required to obtain additional express prior consent from the *retail client* in respect of each instance of *qualifying cryptoasset staking* that the *firm* arranges from time to time using the

retail client's qualifying cryptoassets as part of that agreed auto-staking arrangement.

Key terms

10.3.4 R The terms in respect of which a *firm* must obtain a *retail client's* express prior consent include:

(1) the type and quantity of the *qualifying cryptoassets* the *firm* will use in the *qualifying cryptoasset staking* service for the *retail client*, including the name of the *qualifying cryptoasset* and the blockchain on which *blockchain validation* using that *qualifying cryptoasset* will take place;

(2) how long the *qualifying cryptoassets* will be used in the *qualifying cryptoasset staking* service;

(3) the value of the *qualifying cryptoassets* the *firm* will use in the *qualifying cryptoasset staking* service;

(4) the total and component parts of one-off and ongoing charges, fees and commission, including exit fees, to be paid by the *retail client* to the *firm* for the *qualifying cryptoasset staking* service;

(5) the rewards that may be earned pursuant to the *qualifying cryptoasset staking* service and transferred to the *retail client*, including:

(a) how rewards are determined;

(b) in what *qualifying cryptoasset* or currency the rewards will be paid;

(c) the frequency with which any rewards are earned and whether the value or frequency of rewards is variable; and

(d) whether the *firm* will use any rewards earned in any separate or additional *qualifying cryptoasset staking*;

(6) any restrictions set by the *firm* on a *retail client's* ability to access their *qualifying cryptoassets* used in the *qualifying cryptoasset staking* service or to have the *qualifying cryptoasset* returned to them, and on their ability to access any rewards earned, including whether any financial penalties may be incurred by the *retail client*;

(7) whether ownership of the *retail client's qualifying cryptoassets* transfers from the *retail client* to the *firm* or any other *person* as part of the *qualifying cryptoasset staking* service;

(8) whether the *retail client's qualifying cryptoassets* used in the *qualifying cryptoasset staking* service and/or any rewards earned are

being safeguarded by the *firm* or any other person on behalf of the *retail client*;

(9) what the *retail client's* rights are to cancel or withdraw from the *qualifying cryptoasset staking* service, including:

(a) any relevant information on the conditions for exercising the right of cancellation, its duration, and practical instructions for exercising it; and

(b) any other information material to a *retail client's* understanding in respect of the cancellation of the *qualifying cryptoasset staking* service;

(10) the type and quantity of any *cryptoasset(s)* that the *retail client* may receive as part of the *qualifying cryptoasset staking* service; and

(11) whether any such *cryptoasset(s)* referred to in (10) received by the *retail client* as part of the *qualifying cryptoasset staking* service confer(s) or represent(s) any rights (including ownership) or obligations with respect to the *qualifying cryptoassets* used in the *qualifying cryptoasset staking* service.

10.3.5 R (1) Where the *qualifying cryptoasset staking* service involves auto-staking, in addition to those terms set out in *CRYPTO* 10.3.4R, the terms in respect of which a *firm* must obtain a *retail client's* express prior consent must include:

(a) that the *firm* will use future holdings of one or more types of *qualifying cryptoassets* designated by the *retail client* without needing to seek the *retail client's* express prior consent in respect of each instance of *qualifying cryptoasset staking*; and

(b) the type(s) of *qualifying cryptoasset(s)* the *firm* will use in the *qualifying cryptoasset staking* service for the *retail client*, including the name of the *qualifying cryptoasset(s)* and the associated blockchain(s) or other network(s) on which the *qualifying cryptoasset(s)* will be used for *blockchain validation*.

(2) A *firm* does not need to obtain the *retail client's* express prior consent in relation to:

(a) *CRYPTO* 10.3.4R(1) in respect of the quantity of *qualifying cryptoassets* that will be used in the *qualifying cryptoasset staking* service; and/or

(b) *CRYPTO* 10.3.4(R)(3) in respect of the value of the *qualifying cryptoassets*,

if it is not possible at the outset of the auto-staking service to determine and this.

10.3.6 G (1) In relation to *CRYPTO* 10.3.4R(3), a *firm* should take all reasonable steps to obtain the most recent valuation for the *qualifying cryptoassets* that the *firm* will use in the *qualifying cryptoasset staking* service.

(2) This value in (1) should be presented in GBP.

10.3.7 R (1) In relation to *CRYPTO* 10.3.4R(4), a *firm* should:

(a) make clear which charges originate from the blockchain, such as gas fees, and which charges are levied by the *firm*; and

(b) present any commission charged by the *firm* as a percentage of the total rewards earned on a *retail client's qualifying cryptoasset(s)* used in the *qualifying cryptoasset staking* service.

(2) Where the *qualifying cryptoasset staking* service uses a specified quantity of *qualifying cryptoasset(s)*, a *firm* should present one-off charges for the *qualifying cryptoasset staking* service as monetary value and as a percentage of the total value of *qualifying cryptoasset(s)* used in the *qualifying cryptoasset staking* service.

(3) Where the *qualifying cryptoasset staking* service involves auto-staking, a *firm* should present one-off charges for the use of a *retail client's* future holdings of *qualifying cryptoassets* in *qualifying cryptoasset staking* as either:

(a) a percentage of the total value of *qualifying cryptoassets* used in the *qualifying cryptoasset staking* service; or

(b) a flat charge,

depending on the methodology used by the *firm* to calculate the charges.

Material changes

10.3.8 R A *firm* must notify a *retail client* in good time about any material change to the key terms of agreement provided under *CRYPTO* 10.3.1R(1) relevant to the *qualifying cryptoasset staking* service that the *firm* is providing to that *retail client*.

10.3.9 G When considering its approach to preparing and providing key terms of agreement and obtaining express prior consent in respect thereof, as well as its approach to notifications about material changes to key terms, a *firm* should take into account obligations in the *Handbook* that may be relevant, including but not limited to the *Consumer Duty* and obligations elsewhere in

PRIN and in *COBS*, as well as obligations in consumer rights law and any associated and applicable guidance.

10.4 Notification requirement

10.4.1 R (1) A *firm* must provide a notification to a *retail client*:

(a) within 12 *months* of the *retail client* providing consent pursuant to *CRYPTO* 10.3.1R; and

(b) within 12 *months* of the last notification provided to the *retail client* under this section.

(2) The notification in (1) must include:

(a) all information on the *qualifying cryptoasset staking* service that the *firm* would have provided pursuant to *CRYPTO* 10.2.1R;

(b) the key terms that govern the *qualifying cryptoasset staking* service, which may include only those key terms in respect of which the *firm* obtained the *retail client's* express prior consent pursuant to *CRYPTO* 10.3.1R or may include terms in respect of which material changes have been made during the course of the agreement;

(c) a list of *qualifying cryptoassets*, and the quantity of each, being used for *qualifying cryptoasset staking* for the *retail client*;

(d) the total rewards earned by the *retail client* as part of the qualifying cryptoasset staking service in the past 12 *months*, or from the start of the *qualifying cryptoasset staking* service if less than 12 *months*, presented either as the quantity of qualifying cryptoassets or in GBP; and

(e) the total fees and charges deducted over the past 12 *months*, or since the start of the *qualifying cryptoasset staking* service if less than 12 *months*, presented either as the quantity of qualifying cryptoassets or in GBP.

(3) The content of the notification in (1) must be as up-to-date as possible and the *firm* must state the date on which the information was correct.

10.4.2 G (1) A *firm* should consider whether it may be in the best interests of the *retail client* to provide the notification in *CRYPTO* 10.4.1R(1) sooner than 12 *months* from the point at which the *firm* obtained the *retail client's* express prior consent.

(2) Scenarios in which it may be in the best interests of the *retail client* to provide the notification sooner may include but are not limited to:

(a) where the information needs of the *retail client* may be greater due to increased complexity arising from the nature of the *qualifying cryptoasset staking* service;

(b) where a *retail client* has not, for a significant period, accessed the online system (where provided by the *firm*) through which the *retail client* can view information about the *qualifying cryptoasset staking* service; and/or

(c) where, as a result of one or more material changes having been made or proposed to the agreement, the *firm* considers that it would be in the *retail client's* best interests to notify them sooner.

10.4.3 R A *firm* must provide the notification required by *CRYPTO* 10.4.1R(1) in a *durable medium* or via a website, mobile application or any other digital medium that the *firm* may be using in relation to the provision of its *qualifying cryptoasset staking* service (where it does not constitute a *durable medium*) where the *website conditions* are satisfied.

10.5 Record keeping requirements

10.5.1 R The provisions in this section apply to an *authorised cryptoasset firm* when *arranging qualifying cryptoasset staking* for a *client*.

10.5.2 G For the purposes of this section, references to a '*client*' need only include a *client* whose identity is known to the *firm*.

10.5.3 R (1) A *firm* must maintain records of the following:

(a) the amount of *qualifying cryptoassets* used in a *qualifying cryptoasset staking* service for each *client* and on which blockchain, per day;

(b) whether the *qualifying cryptoassets* used in *qualifying cryptoasset staking* are safeguarded for the *client* by or on behalf of the *firm* and, if by another *person*, by whom;

(c) the total amount of rewards earned in relation to each *client's qualifying cryptoasset* per day;

(d) the total amount of rewards allocated to each *client* per day;

(e) total fees, charges or commissions charged to each *client* per day;

(f) for each *client*, the type and quantity of *qualifying cryptoassets* provided to the *client* which the *client* may need to return to or exchange with the *firm* or another *person* for the return of the

qualifying cryptoassets being used in a *qualifying cryptoasset* service, and the return of any rewards (where applicable);

(g) where applicable, the key terms of agreement provided to each *client* and each *client's* express prior consent provided in relation thereto, including the date, time and – where specified in the agreement – the quantity of *qualifying cryptoassets* used in the *qualifying cryptoasset staking* service;

(h) all requests from *clients* to terminate the *qualifying cryptoasset staking* service or for the *client's qualifying cryptoassets* to be returned, including the date, time and amount of *qualifying cryptoassets* requested to be returned;

(i) a record of *qualifying cryptoasset staking* activation, including the date, time and amount of *qualifying cryptoassets* used in a *qualifying cryptoasset staking* service;

(j) a record of *qualifying cryptoasset staking* completion, including the date, time and amount of *qualifying cryptoassets* that are capable of being returned to the *client*;

(k) the total amount of *qualifying cryptoassets* used in the *qualifying cryptoasset staking* service lost per day due to operational disruptions;

(l) all notifications provided to the *retail client* pursuant to *CRYPTO* 10.2.4R;

(m) all notifications provided to the *retail client* pursuant to *CRYPTO* 10.3.8R; and

(n) all notifications provided to the *retail client* pursuant to *CRYPTO* 10.4.1R.

(2) Subject to (3), all records in (1) must be retained for a period of 5 years from the point at which the record is generated.

(3) The records in (1)(g) and (1)(l) to (n) must be retained for a period of at least 5 years from the point at which the record is generated or for the duration of the relationship with the *client*, whichever is longer.

10.5.4 G For the purposes of *CRYPTO* 10.5.3R(1)(i), '*qualifying cryptoasset staking* activation' refers to the point at which *qualifying cryptoassets* are used in the *blockchain validation* process.

10.5.5 G For the purposes of *CRYPTO* 10.5.3R(1)(j), '*qualifying cryptoasset staking* completion' refers to the cessation of the *blockchain validation* process and restoration of the same access over *qualifying cryptoassets* that the *client* had before the commencement of the *qualifying cryptoasset staking* service.

10.6 Obligations in COBS

10.6.1 G A *firm* may satisfy its obligations under this chapter and any other applicable provisions in *COBS* by means of a single set of systems, controls, policies, procedures, communications or contractual arrangements, provided that those arrangements, taken as a whole, meet the requirements of each applicable provision in this chapter and COBS.

10.6.2 G The purpose of this section is to avoid unnecessary duplication of systems, controls and client interactions where a *firm* is subject to overlapping requirements under this chapter and other *COBS* provisions.

CRYPTOASSETS (SAFEGUARDING) 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 powers and related sections in the Financial Services and Markets Act 2000 ("the Act"):

(a) section 137A (The FCA's general rules);
(b) section 137T (General supplementary powers);
(c) section 138D (Actions for damages); and
(d) section 139A (Power of the FCA to give guidance); and

(2) the other powers and related provisions listed in Schedule 4 (Powers exercised) to the General Provisions of the FCA's Handbook.

B. The rule-making provisions listed above are specified for the purposes 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 Consequentials) Instrument 2026;
(10) Cryptoassets (Conduct and Firm Standards) Instrument 2026; and
(11) Cryptoassets (COREPRU and CRYPTOPRU) Instrument 2026.

Amendments to the Handbook

D. The Client Assets sourcebook (CASS) is amended in accordance with the Annex to this instrument.

Notes

E. In the Annex to this instrument, the notes (indicated by "*Editor's note*:") are included for the convenience of readers but do not form part of the legislative text.

Citation

F. This instrument may be cited as the Cryptoassets (Safeguarding) Instrument 2026.

By order of the Board
25 June 2026

Annex

Amendments to the Client Assets sourcebook (CASS)

In this Annex, underlining indicates new text and striking through indicates deleted text, unless otherwise stated.

6 Custody rules

6.1 Application

6.1.1 R This chapter (the *custody rules*) applies to a *firm*:

…

(1B) when ~~it is *safeguarding and administering investments*~~, in the course of business that is not *MiFID business*~~;~~, it is:

(a) *safeguarding and administering investments*;

(b) *safeguarding cryptoassets* which are *relevant specified investment cryptoassets* and which do not belong to the *firm*; or

(c) *arranging cryptoasset safeguarding* in relation to *relevant specified investment cryptoassets*;

…

[*Editor's note*: CASS 6.1.1-AR is deleted and has been moved to CASS 6.1.1-DR.]

6.1.1-A R ~~In applying the *custody rules* to a *small AIFM's excluded custody activities*, any reference to a *firm* carrying on the *regulated activities* of *safeguarding and administering investments*, *safeguarding and administering assets (without arranging)* or *arranging safeguarding and administration of assets* includes those *excluded custody activities* that would, but for the exclusion in article 72AA of the *RAO*, amount to whichever of those *regulated activities* is referred to.~~ [deleted]

6.1.1-B R (1) In applying the *custody rules* to a *firm's* activities under *CASS* 6.1.1R(1B)(b) or *CASS* 6.1.1R(1F), any reference in the *custody rules* to *safeguarding and administering investments* or *safeguarding and administration of assets (without arranging)* should be read as including *safeguarding cryptoassets* which are *relevant specified investment cryptoassets*.

(2) In applying the *custody rules* to a *firm's* activities under *CASS* 6.1.1R(1B)(c), any reference the *custody rules* to *arranging safeguarding and administration of assets* should be read as

including *arranging cryptoasset safeguarding* in relation to *cryptoassets* which are *relevant specified investment cryptoassets*.

6.1.1-C G (1) The effect of *CASS* 6.1.1-BR is to extend the requirements in the *custody rules* to *safeguarding cryptoassets* and *arranging cryptoasset safeguarding*, in either case in so far as they relate to *relevant specified investment cryptoassets*.

(2) This has the effect that, for the purposes of applying the *custody rules* (but for no other purposes):

(a) the provision at Article 40(4) of the *RAO* inserted by Article 40(6) of SI 2026/102 should be disregarded; and

(b) even where the *firm* is not providing any 'administration' services for the *relevant specified investment cryptoassets* in respect of which it is *safeguarding cryptoassets*, the requirements of the *custody rules* would still apply to it in relation to that *safeguarding cryptoassets* activity.

(3) *CASS* 6.1.1-BR should be read as altering the meaning of any *Glossary* definition that is relevant to interpreting the *custody rules*, as well as altering the scope of the requirements in those *rules*.

(4) The reference to a *small AIFM's excluded custody activities* in *CASS* 6.1.1R(1F) is also affected by *CASS* 6.1.1-BR(1). This means that *CASS* 6 applies to a *small AIFM's* activity of *safeguarding cryptoassets* which are *relevant specified investment cryptoassets* despite the exclusion in article 72AA of the *RAO*.

6.1.1-D R In applying the *custody rules* to a *small AIFM's excluded custody activities*, any reference to a *firm* carrying on the *regulated activities* of *safeguarding and administering investments*, *safeguarding and administering assets (without arranging)* or *arranging safeguarding and administration of assets* includes those *excluded custody activities* that would, but for the exclusion in article 72AA of the *RAO*, amount to whichever of those *regulated activities* is referred to.

Insert the following new chapter, CASS 17, after CASS 16 (Stablecoin backing assets). All the text is new and is not underlined.

17 Cryptoasset safeguarding rules

17.1 Application

17.1.1 R Subject to *CASS* 17.1.3R, this chapter (the *cryptoasset safeguarding rules*) applies to a *firm* in relation to *regulated activities* carried on by it from an *establishment* in the *UK*.

17.1.2 G (1) Specific sections within the *cryptoasset safeguarding rules* have a narrower application than that set out in *CASS* 17.1.1R.

(2) *CASS* 17.3 (Cryptoasset safeguarding trusts) applies to a *firm* when it is *safeguarding cryptoassets*. The *rule* at *CASS* 17.3.3R requires the *firm* to act as a trustee when it is *safeguarding cryptoassets*, subject to certain exceptions which are set out in subsequent *rules* in that section. The *rule* at *CASS* 17.3.20R permits the *firm* to hold other *cryptoassets* within the same trust or trusts, as an *operational surplus*, and subject to certain conditions. *Cryptoassets* that are required or permitted to be in trust under those provisions of *CASS* 17.3 (Cryptoasset safeguarding trusts) are termed '*client cryptoassets*' in the *cryptoasset safeguarding rules*.

(3) *CASS* 17.2 (General safeguarding requirements), *CASS* 17.4 (Means of access) and *CASS* 17.5 (Records of cryptoassets and reconciliations) apply to a *firm* when it is, as a trustee under *CASS* 17.3.3R, *safeguarding cryptoassets* which are *client cryptoassets* (and therefore including any *operational surplus* that is permitted under *CASS* 17.3.20R).

(4) In addition, *CASS* 17.2 (General safeguarding requirements) and *CASS* 17.4 (Means of access) apply to a *firm* when it is *safeguarding cryptoassets* but not treating them as *client cryptoassets*, in reliance upon *CASS* 17.3.12R.

(5) *CASS* 17.6 (Appointing third parties to safeguard cryptoassets) applies to a *firm* when it is both *safeguarding cryptoassets* and *arranging cryptoasset safeguarding* in relation to the same *client cryptoassets*.

(6) *CASS* 17.7 (Arranging cryptoasset safeguarding) applies to a *firm* when it merely *arranges cryptoasset safeguarding*.

17.1.3 R This chapter does not apply to a *UK QCATP operator* which is an *overseas firm* and whose *Part 4A permission* for *cryptoasset safeguarding* is subject to a *requirement* (or a requirement imposed under section 55L(5) of the *Act*) to:

(1) not carry on the *regulated activity* of *cryptoasset safeguarding* other than by having control of *qualifying cryptoassets* to facilitate the settlement of transactions executed on a *UK QCATP*; and

(2) in the course of carrying on the *regulated activity* of *cryptoasset safeguarding* in accordance with (1), not accept any *qualifying cryptoassets* from any *UK* user other than *qualifying cryptoassets* received via a member of its *group* who is subject to, and acting in accordance with, *CASS* 17.3.5R.

17.1.4 G (1) The exemption at *CASS* 17.1.3R permits a *UK QCATP operator* whose settlement arrangements would involve the *regulated activity* of *cryptoasset safeguarding* (for example, because users of the *UK QCATP* have a right against the *UK QCATP operator* for the

return of *cryptoassets*) to not have to treat *qualifying cryptoassets* which it controls as part of those settlement arrangements as *client cryptoassets*.

(2) The exemption at *CASS* 17.1.3R only applies to a *UK QCATP operator* if its *Part 4A permission* is subject to a requirement, either at the *FCA's* own initiative or following the voluntary application by the *firm*, in the terms set out at *CASS* 17.1.3R(1) and (2).

(3) The effect of the part of that *requirement* which is set out at *CASS* 17.1.3R(2), together with *CASS* 17.3.5R, is to limit the amount of *qualifying cryptoassets* which would be owed to *UK* users in respect of which *CASS* 17 would not apply.

17.1.5 G (1) The defined term '*cryptoasset safeguarding class*' is an important concept in the *cryptoasset safeguarding rules* and *rules* related to *safeguarding cryptoassets* (for example, in the reporting requirements at *SUP* 16.35.7R). Examples and further *guidance* to show the effect of this term are set out below.

(2) For example, two *qualifying stablecoins* which are both instances of the same *qualifying stablecoin product* should not, for the purpose of the *cryptoasset safeguarding rules* and *rules* related to *safeguarding cryptoassets*, be considered to be in the same '*cryptoasset safeguarding class*' unless they exist on the same network that uses distributed ledger technology (eg, blockchain).

(3) Similarly, two *qualifying cryptoassets* should not be considered as falling within the same '*cryptoasset safeguarding class*' unless they are both instances of the same single product. This means that a *wrapped token* or a liquid staking token would not fall within the same '*cryptoasset safeguarding class*' as the relevant underlying *cryptoasset*.

(4) A consequence of this is likely to be that if a *firm* is carrying on *safeguarding cryptoassets* in relation to a *client cryptoasset* of a particular *cryptoasset safeguarding class*, it would not, without the *client's* agreement, be able to discharge its *safeguarding* obligations to its *client* by returning a *cryptoasset* that is identical to the one being *safeguarded* but for the fact that it exists on a different blockchain.

(5) Where the *cryptoasset safeguarding rules* require a *firm* to make a record or a notification that refers to a *cryptoasset safeguarding class*, the *firm* may be able to use the Digital Token Identifier system outlined in ISO standard 24165, provided that, in doing so, the relevant *cryptoasset safeguarding class* can be precisely distinguished.

Requirement to act compatibly with the Consumer Duty

17.1.6 R (1) When applying the *cryptoasset safeguarding rules* in relation to a *firm's retail market business*, the *firm* must act compatibly with the *Consumer Duty*.

(2) A contravention of (1) does not give rise to a right of action by a *private person* under section 138D of the *Act* (and *CASS* 17.1.6R(1) is specified under section 138D(3) of the *Act* as a provision giving rise to no such right of action).

Exception for relevant specified investment cryptoassets

17.1.7 R This chapter (the *cryptoasset safeguarding rules*) does not apply to a *firm* in relation to any *safeguarding cryptoassets* activity or any *arranging cryptoasset safeguarding* activity where the *cryptoassets* in respect of which the *firm* is carrying on *safeguarding cryptoassets* or *arranging cryptoasset safeguarding* (as applicable) are *relevant specified investment cryptoassets*.

17.2 General safeguarding requirements

17.2.1 R This section applies to a *firm* when it is:

(1) *safeguarding cryptoassets* which are *client cryptoassets*; or

(2) *safeguarding cryptoassets* which would be *client cryptoassets* but are not being treated by the *firm* as *client cryptoassets* in reliance upon *CASS* 17.3.12R.

Requirement for adequate organisational arrangements

17.2.2 R A *firm* must, when *safeguarding cryptoassets*, introduce and maintain adequate organisational arrangements to:

(1) protect the relevant *client's* rights in relation to the *cryptoassets*, including in the event of the *firm's* insolvency; and

(2) minimise the risk of the loss or diminution of the *cryptoassets*, or of the rights in connection with those *cryptoassets*, as a result of the misuse of the *cryptoassets*, fraud, poor administration, inadequate record-keeping or negligence.

17.3 Cryptoasset safeguarding trusts

17.3.1 R This section applies to a *firm* when it is *safeguarding cryptoassets*.

Context and purpose

17.3.2 G (1) The scope of the *regulated activity* of *safeguarding cryptoassets* covers a range of legal relationships between the *firm* and the *client* in relation to a *qualifying cryptoasset* or *relevant specified investment cryptoasset*. It does not only apply where a *cryptoasset* that is controlled by a *firm* belongs to a *client*.

(2) Where the other conditions of the scope of the activity are met, the *regulated activity* of *safeguarding cryptoassets* is carried on in cases where the *person* on whose behalf the *firm* is safeguarding is the beneficial owner of the *cryptoasset*, and also in certain cases where that *person* has a right against the *firm* for return of a *cryptoasset*. The scope of the *regulated activity* for the latter type of case (where that *person* has a right for return) depends on whether the *firm* and that *person* have entered into a 'title transfer collateral arrangement' or repurchase agreement and on whether that *person* is a 'consumer' (as those terms are defined at Article 9N(5) of the *RAO*).

(3) The purpose of this section is to:

(a) set out a general requirement which would prohibit a *firm* from carrying on the *regulated activity* of *safeguarding cryptoassets* under any of those sorts of legal relationships that are within the scope of that *regulated activity* other than as a trustee;

(b) provide certain exemptions to that requirement to act as a trustee, subject to particular conditions being met; and

(c) set out other more specific requirements which a *firm* must meet when that requirement to act as a trustee applies.

(4)

(a) In the following *guidance*, the *FCA* sets out its policy rationale for the requirements and exemptions in this section concerning trusts.

(b) It is important that, in line with the requirements in *CASS* 17.2, *clients'* rights to *cryptoassets* which are being *safeguarded* are adequately protected through the use of trusts which can withstand competing claims to those *cryptoassets*, for example in case of the insolvency of the *firm* which is carrying on the *regulated activity* of *safeguarding cryptoassets*. In the *FCA's* view, this has market integrity advantages in the context of section 1D of the *Act*.

(c) Furthermore, in the *FCA's* view, taking account of potential difficulties that a *client* may have in evidencing and asserting ownership claims to *cryptoassets* (particularly where the *firm* has full control over those *cryptoassets*), a trust arrangement has consumer protection advantages over other legal arrangements that might exist between a *client* and *firm* in the context of *safeguarding cryptoassets* (such as an absolute title transfer or an agency arrangement), in the context of section 1C of the *Act*.

(d) This general requirement to *safeguard cryptoassets* as a trustee is set out at *CASS* 17.3.3R.

(i) That *rule* requires a *firm* to agree with its *client* that the *firm* will act as a trustee, so that this should clear to the *client*.

(ii) That *rule* does not create a statutory trust; the *FCA* is of the view that *firms* to which that requirement applies should have some flexibility around how they create private trusts, subject to certain conditions being met (see *CASS* 17.3.14R to *CASS* 17.3.18G).

(iii) Detailed and up-to-date records are also mandatory (see *CASS* 17.3.19R).

(e) However, certain other services which *clients* may engage a *firm* which is carrying on the *regulated activity* of *safeguarding cryptoassets* to provide in relation to *cryptoassets* would not be compatible with *cryptoassets* being *safeguarded* on trust. This is provided for at:

(i) *CASS* 17.3.4R in relation to *qualifying cryptoasset lending*;

(ii) *CASS* 17.3.5R in relation to the settlement of transactions executed on a *UK QCATP*; and

(iii) *CASS* 17.3.6 in relation to other services.

(f) In addition, a *firm* may be released from the requirement to act as a trustee where its dealings with the relevant *client* would require that. This is provided for at:

(i) *CASS* 17.3.8R in relation to a *client's* instructions to transfer a *cryptoasset* to another *person* (including the *firm*); and

(ii) *CASS* 17.3.10R in relation to a *client's* indebtedness to the *firm*.

(g) Furthermore, the *FCA* is of the view that it is disproportionate to require a *firm* to be a trustee where it is engaged to only provide a backup solution where its *client* contemporaneously retains full control of the *cryptoasset* in question. This is provided for at *CASS* 17.3.12R.

(h) *Firms* should note that each of the exemptions referred to above are subject to conditions set out within those *rules*.

(i) Finally, and again provided certain conditions are met including that this is necessary in order to service *clients*, a *firm* may co-mingle 'house' *cryptoassets* in the same trust as *client cryptoassets*. See *CASS* 17.3.20R on *operational surpluses*.

Requirement to safeguard as a trustee

17.3.3 R (1) Unless otherwise permitted in this section, a *firm* must ensure that wherever it carries on the *regulated activity* of *safeguarding cryptoassets*, it does so as a trustee of the relevant *cryptoasset* under trust arrangements which comply with *CASS* 17.3.14R.

(2) In so far as the requirement in (1) applies, a *firm* must ensure that its *client* on behalf of whom it is *safeguarding cryptoassets* has agreed to the *firm safeguarding cryptoassets* as a trustee (for example in any written agreement required under *COBS* 8.1 (Client agreements: non-MiFID designated investment business)).

(3) A *firm* must ensure that its *client's* agreement under (2) addresses how the trust is to be established (for example in relation to legal title transferring to the *firm* pursuant to a transfer of the *cryptoasset* to the *firm's* control).

Exemption from acting as a trustee for cryptoasset lending

17.3.4 R (1) A *firm* is not required to *safeguard cryptoassets* as a trustee under *CASS* 17.3.3R or, if it is already carrying on *safeguarding cryptoassets* in respect of a *client cryptoasset* as a trustee under *CASS* 17.3.3R, the *firm* may cease to treat a *cryptoasset* as a *client cryptoasset*, where the *client* on behalf of whom the *firm* is carrying on *safeguarding cryptoassets* has engaged the *firm* to provide a *qualifying cryptoasset lending* service in relation to a *cryptoasset*.

(2) The exemption in (1) only applies during the period for which the *qualifying cryptoasset lending* service is being provided in relation to that *cryptoasset*.

(3) Once that *qualifying cryptoasset lending* service in relation to a *cryptoasset* has ended for any reason, including by prior agreement or if the *client* has exercised any right to require that service to cease in relation to a *cryptoasset*, the exemption in (1) no longer applies.

(4) A *firm* may not use the exemption in (1) in relation to any *cryptoasset* which represents *qualifying cryptoasset borrowing collateral*, whether the obligations which the *cryptoasset* secures are owed to the *firm* itself or to another *authorised person* who has, under *CRYPTO* 9.6.8R(1)(b), arranged for the *firm* to carry on the *regulated activity* of *safeguarding cryptoassets*.

Exemption from acting as a trustee for qualifying cryptoasset trading platforms

17.3.5 R A *firm* may cease to treat a *qualifying cryptoasset* as a *client cryptoasset* (and therefore cease to carry on *safeguarding cryptoassets* as a trustee of the *cryptoasset*) where:

(1) the *client* on behalf of whom the *firm* is *safeguarding* the *qualifying cryptoasset* is also a user of a *UK QCATP* operated by the *firm* itself or another *person* in the *firm's group*;

(2) that *client* is trading, or has made it clear to the *firm* that they intend to trade, with *qualifying cryptoassets* of that *cryptoasset safeguarding class* using that *UK QCATP*;

(3) as part of the day-to-day operation of that *UK QCATP*, the *UK QCATP operator* needs to take control of *qualifying cryptoassets* to facilitate the settlement of transactions executed on that *UK QCATP*;

(4) the *firm* has obtained the *client's* prior informed consent, in accordance with *CASS* 17.3.11R, to the *qualifying cryptoasset* ceasing to be a *client cryptoasset* in order for transactions executed on the *UK QCATP* in that *cryptoasset safeguarding class* to settle; and

(5) at all times, the amount of *cryptoassets* of a particular *cryptoasset safeguarding class* which the *firm* is not treating as *client cryptoassets* under this *rule* for the *client* does not exceed 2% of the total amount of *cryptoassets* of that particular *cryptoasset safeguarding class* which remain in the *firm's* trusteeship for that *client* under *CASS* 17.3.3R.

Exemption from acting as a trustee where necessary for other services

17.3.6 R (1) A *firm* is not required to *safeguard cryptoassets* as a trustee under *CASS* 17.3.3R or, if it is already carrying on *safeguarding cryptoassets* in respect of a *client cryptoasset* as a trustee under *CASS* 17.3.3R, the *firm* may cease to treat that *cryptoasset* as a *client cryptoasset*, where:

(a) the *client* on behalf of whom the *firm* is carrying on *safeguarding cryptoassets* has engaged the *firm* to provide a service (other than services described in *CASS* 17.3.4R or *CASS* 17.3.5R);

(b) in order to provide that service to the *client*, the *firm* has concluded that it is necessary:

(i) for the *firm* to have ownership of the *cryptoasset*; and/or

(ii) for the *firm* to effect a transfer of ownership of the *cryptoasset* to another *person*; and

(c) the *firm* has obtained the *client's* prior informed consent, in accordance with *CASS* 17.3.11R, to that transfer of ownership in order for the service to be provided.

(2) Where a service for which the *firm* has relied on (1) ends, or where it is no longer necessary for the *firm* or another *person* to have ownership of *cryptoassets*, the exemption in (1) no longer applies.

(3) For each distinct service for which the *firm* intends to rely on (1), and prior to providing that service to any *client*, the *firm* must make a record of the reasons for concluding that it is necessary for the *firm* to have ownership of *cryptoassets*, or to effect a transfer of ownership of *cryptoassets* to another *person*, in order to provide that service (the '*client cryptoasset trust exemption record*').

(4) For the purposes of (3), a service must be considered 'distinct' if it has different technical features, a different purpose, or a different type of risk to the *client* to a service which has already been assessed by the *firm*.

(5) The *firm* must retain each *client cryptoasset trust exemption record* made under (3) for a period of 5 years after it has stopped providing the relevant service.

(6) A *firm* may not use the exemption in (1) in relation to any *cryptoasset* which represents *qualifying cryptoasset borrowing collateral*, whether the obligations which the *cryptoasset* secures are owed to the *firm* itself or to another *authorised person* who has, under *CRYPTO* 9.6.8R(1)(b), arranged for the *firm* to carry on the *regulated activity* of *safeguarding cryptoassets*.

17.3.7 G (1) The reference to 'distinct' service in *CASS* 17.3.6R(3) should be interpreted on a granular basis, meaning that a *firm* should investigate and conclude that a transfer of ownership is necessary in relation to the specific features of the service. For example, if a *firm* intends to rely on *CASS* 17.3.6R(1) in order to carry on the activity of *arranging qualifying cryptoasset staking*, it should make a record under *CASS* 17.3.6R(3) for each staking protocol in relation to which it will provide services.

(2) For the purposes of *CASS* 17.3.6R(1), the term 'service' should not be limited to services which only comprise *regulated activities*.

Exemption from acting as a trustee to act on client instructions to transfer

17.3.8 R A *firm* may cease to treat a *cryptoasset* as a *client cryptoasset* where:

(1) the relevant *client* has given the *firm* an express and specific instruction to effect a transfer of an amount or value of their *client cryptoassets* to another *person*, to the *firm* or to the *client* themselves; and

(2) the *firm* has given effect to that instruction.

17.3.9 G (1) The reference to an 'express and specific instruction' at *CASS* 17.3.8R(1) means that the *rule* cannot be relied on where the *client* has given the *firm* a mandate in relation to their *client cryptoassets* without any specific instruction for any particular transfer (for example, a discretionary investment mandate). For such a service where there is no express and specific *client* instruction, a *firm* may be able to rely on *CASS* 17.3.6R provided that the conditions in that *rule* are met.

(2) Following a transfer under *CASS* 17.3.8R to another *person* (the 'transferee'), the *firm* would be required to continue to *safeguard cryptoassets* in accordance with the requirements in this section if it is carrying on the *regulated activity* of *safeguarding cryptoassets* on behalf of the transferee in relation to that *cryptoasset*. This may mean that the *firm* will be required to *safeguard cryptoassets* as a trustee on behalf of the transferee.

Exemption from acting as a trustee where the client is indebted to the firm

17.3.10 R A *firm* may cease to treat a *cryptoasset* as a *client cryptoasset* where:

(1) the relevant *client* has given the *firm* a right, through a written binding agreement, to take ownership of their *cryptoassets* in order to discharge an obligation that the *client* owes to the *firm*; and

(2) the *firm* has exercised that right in accordance with the terms of that written agreement in relation to those *client cryptoassets*.

Obtaining a client's consent

17.3.11 R (1) This *rule* sets out steps which a *firm* must take in the course of obtaining a *client's* prior informed consent under *CASS* 17.3.5R(4) or *CASS* 17.3.6R(1)(c).

(2) For any *retail market business*, the *firm's* process for obtaining prior informed consent must be compatible with the *Consumer Duty*.

(3) In the course of seeking consent, the *firm* must specifically and clearly explain to the *client* the risks to the *client* of the *cryptoasset* not being within a trust, including in the event of the *firm's failure*.

(4) Any consent provided by a *client* must be obtained in writing and a record of it (the '*client cryptoasset trust exemption consent record*') must be retained for a period of 5 years after the *firm* has stopped relying on the consent to use the exemption at *CASS* 17.3.5R(1) or *CASS* 17.3.6R(1), as applicable.

(5) If a *client* withdraws their consent, the *firm* can no longer rely on the exemption at *CASS* 17.3.5R(1) or *CASS* 17.3.6R(1), as applicable, from the time at which the *client's* withdrawal of consent takes effect (taking into account any agreed notice period).

(6) A contravention of (2) does not give rise to a right of action by a private person under section 138D of the *Act* (and *CASS* 17.3.11R(2) is specified under section 138D(3) of the *Act* as a provision giving rise to no such right of action).

(7) A contravention of any other aspect of this *rule* is not affected by (6).

Exemption from acting as a trustee where providing a backup solution

17.3.12 R A *firm* is not required to *safeguard cryptoassets* as a trustee under *CASS* 17.3.3R where all the following conditions are met:

(1) the *firm* has good reason to believe that the *client* on whose behalf the *firm* is carrying on *safeguarding cryptoassets* in respect of a particular *cryptoasset* has its own *means of access* which would enable the *client* to transact using the *cryptoasset* without relying on the *firm*;

(2) where that *client* is a *firm* that is itself also carrying on *safeguarding cryptoassets* in relation to that *cryptoasset*, that *client* has confirmed to the *firm* to which this *rule* applies that it is itself carrying on *safeguarding cryptoassets* in respect of that *cryptoasset* as a trustee under *CASS* 17.3.3R (as it applies to that *client*);

(3) the *firm* has not been appointed to provide any service in relation to that *cryptoasset* other than:

(a) undertaking one or more of the activities set out at *CASS* 17.4.2R in relation to the relevant *means of access* to the *cryptoasset* for which it is carrying on *safeguarding cryptoassets*; and

(b) undertaking those activities at *CASS* 17.4.2R only for the purposes of assisting the *client* in the event that the *client's* own *means of access* becomes lost, inoperable, inaccessible or irrecoverable; and

(4) when carrying on that limited *safeguarding cryptoassets* service, the *firm* does not also carry on the activity of *arranging cryptoasset safeguarding* in relation to that *cryptoasset*.

17.3.13 G (1) It may be possible for a *firm* to rely on the exemption at *CASS* 17.3.12R where it has been appointed to provide a backup and recovery solution for a *client* (and no other service).

(2) The *client* in the situation described in (1) may itself be another *firm* (or an unauthorised *cryptoasset* service provider) which has engaged the *firm* to provide that backup and recovery solution in order to make its own service more robust. The condition at *CASS* 17.3.12R(2) is only relevant where the *client* is a is another *firm* which is itself carrying on *safeguarding cryptoassets* in respect of the relevant *cryptoasset*.

(3) Where the *client* is another *firm* which is not carrying on *safeguarding cryptoassets* in respect of the relevant *cryptoasset* (for example, because it owns the *cryptoasset* outright for the purposes of *dealing in qualifying cryptoassets as principal*, and no other *person* has a right for the return of it) then the condition at *CASS* 17.3.12R(2) would not be relevant.

(4) Likewise, where the *client* is simply the investor in the *cryptoasset* (and provides no service to any other *person*) then the condition at *CASS* 17.3.12R(2) would not be relevant.

(5) To meet the condition at *CASS* 17.3.12R(1), it should not be necessary for the *firm* to prove (cryptographically or otherwise) that the *client* has their own *means of access*, but the *firm* should be able to explain the basis of its belief that the *client* is in that position. For example, this may be a point which is addressed in the *firm's* agreement with the *client*.

(6) The *client's* own *means of access* referred to at *CASS* 17.3.12R(1) may be a duplicate copy of the *firm's means of access* or may be an alternative *means of access* which co-exists with the *firm's means of access*.

Setting up and operating client cryptoasset trusts

17.3.14 R For any *client cryptoasset*, the *firm* must ensure that:

(1) the trust that is required under *CASS* 17.3.3R is created and operated by the *firm* in accordance with applicable legal requirements for trusts in the *UK*;

(2) the terms of any such trust are clearly documented with the effect that it is clear the trust is intended and it is clear what the terms are; and

(3) the terms and operation of the trust by the *firm* deliver the objectives and include the provisions set out in *CASS* 17.3.17R.

17.3.15 G To comply with *CASS* 17.3.14R(2) a *firm* may, for example, execute a deed or similar formal instrument.

17.3.16 R A *firm* must retain any document required under *CASS* 17.3.14R(2) setting out the terms of a trust, and details of any amendments which were made to the terms after the trust was first created, from the point at which the trust is created or the terms of the trust amended, and until 5 years after the trust has been brought to an end.

17.3.17 R A *firm* must ensure that the terms and operation of any trust that is required under *CASS* 17.3.3R deliver the objectives at (1) and (2) and include the provisions at (3) and (4):

(1) The *firm* must act as a trustee in relation to the *client cryptoassets* as well as in relation to any rights which can be exercised by virtue of the *firm safeguarding cryptoassets*, and in particular:

(a) the *firm* must be required to respond to the lawful instructions of the relevant *client* in relation to the *client cryptoassets*; and

(b) save for having the necessary powers to comply with any applicable *rules* or legal requirements, or unless otherwise agreed with the *client*, the *firm* must not have any discretion in applying, investing or otherwise using any *client cryptoassets* which are trust property.

(2) Subject to *CASS* 17.3.20R, the *firm's* operation of the trust ensures that the *client cryptoassets* within the trust are not co-mingled with, and are identifiable separately from, any other assets (for example, any assets for which the *firm* is not carrying on *safeguarding cryptoassets*, any assets for which the *firm* is relying on an exemption to act as a trustee under this section, and any assets which pertain to any other separate trust that is created to meet *CASS* 17.3.3R).

(3) Where there is, or is intended to be, more than one *client* on whose behalf the *firm* is *safeguarding cryptoassets* within a single trust, the terms of that trust must set out how any shortfalls in the trust, whether within a particular *cryptoasset safeguarding class* or across all *cryptoasset safeguarding classes* of *client cryptoassets* within the trust, are to be allocated between the *clients*.

(4) The terms of the trust must set out whether or not the *client cryptoassets* within the trust may be applied towards funding the distribution costs of the trust on the *failure* of the trustee and, if the terms do provide for this, the basis on which that funding will be deducted from the entitlements of the *clients*.

17.3.18 G (1) A *firm* should decide on an approach to settling and operating trusts under the *rules* in this section which is suitable for its business model, its *client* base and the types of *client cryptoassets* in respect of which it will be *safeguarding cryptoassets*. In particular:

(a) a *firm* may decide whether to operate separate trusts for each *client* or one or more 'omnibus' trusts for a particular class of *clients* (which may include all *clients*);

(b) a *firm* may decide whether to operate separate trusts for different *cryptoasset safeguarding classes*; and

(c) a *firm* may decide whether to operate separate trusts distinctly, using separate virtual addresses or devices, or to combine *client cryptoassets* at different virtual addresses or devices into the same trust.

(2) (a) A *firm* should consider whether the objective in *CASS* 17.3.17R(2) can be achieved through the use of different virtual addresses, with regard to the operation of the relevant network.

(b) A particular network relevant to a type of *client cryptoasset* may affect the choices available to a *firm* in deciding how to implement a trust which complies with the *rules* in this section.

(c) Where the network relies on another network for its functioning, a *firm* should ensure that the ownership of the *client cryptoassets* cannot be challenged or reversed through the operation of technology.

(d) Allocating *client cryptoassets* which exist at the same single virtual addresses or on the same single device into different trusts would not meet the requirement at *CASS* 17.3.17R(2) in relation to co-mingling.

(3) (a) A *firm* may decide how any shortfall in a trust should be allocated between *clients*, but in doing so, a *firm* should consider the requirement at *CASS* 17.1.6R.

(b) The *FCA* would generally expect a shortfall in a particular *cryptoasset safeguarding class* within a trust to be borne 'pro rata' by all *clients* for whom the *firm* is safeguarding *cryptoassets* of that particular *cryptoasset safeguarding class* in that particular trust, in proportion to their respective interests in those *cryptoassets*.

(4) The way in which a *firm* decides to set up its trust environment and the way in which it achieves the required segregation should be recorded in the *firm's client cryptoasset trust records*.

The client cryptoasset trust record

17.3.19 R (1) A *firm* must make and keep updated a record of each trust that it has created under *CASS* 17.3.3R which sets out the following details for that trust (the '*client cryptoasset trust record*'):

(a) a unique identifier code for the trust;

(b) the means by which the *firm* achieves the obligation at *CASS* 17.3.17R(2) including, where applicable:

(i) each relevant virtual address or device controlled by the *firm* at which *cryptoassets* pertaining to the trust are being safeguarded by the *firm*;

(ii) the name of each third party who has been appointed to *safeguard cryptoassets* pertaining to the trust under *CASS* 17.6; and

(iii) the identifier of the relevant network for the trust property;

(c) the name of each *client* who has an interest in the trust;

(d) the *cryptoasset safeguarding class(es)*in the trust, identified using the name of the *cryptoasset* or an identification code, in either case from which the relevant *cryptoasset safeguarding class* can be precisely distinguished;

(e) the location of the record of the terms of the trust required under *CASS* 17.3.16R;

(f) whether or not the *firm* has decided for the trust to include an *operational surplus* under *CASS* 17.3.20R; and

(g) if the trust has been brought to an end, the date of that occurring and the reason why it was brought to an end.

(2) A *client cryptoasset trust record* must be made at the same time as the relevant trust is created, and it must be updated immediately:

(a) upon making any changes to that trust; and

(b) as necessary following any *client cryptoasset reconciliation* under *CASS* 17.5.

(3) A *client cryptoasset trust record* must be retained for a period of 5 years after the relevant trust has been brought to an end.

Permitted operational surplus in trusts

17.3.20 R A *firm* may include, within any trust required to be created under *CASS* 17.3.3R, an amount of additional *qualifying cryptoassets* or *relevant specified investment cryptoassets* funded from the *firm's* own resources in order to meet the *firm's* operational needs (an '*operational surplus*'), provided the following conditions are met:

(1) An *operational surplus* in a trust is only permitted if it is necessary in order for the *firm* to provide services to one or more *clients* for whom the *firm* is *safeguarding cryptoassets*.

(2) Subject to (3), the *operational surplus* must be in the same *cryptoasset safeguarding class* as that in relation to which the *firm* is providing the services that necessitate the *operational surplus*.

(3) As an exception to (2), the *operational surplus* may be in a different *cryptoasset safeguarding class* where that would be necessary due to a technical limitation or feature of those services which the *firm* intends to provide.

(4) The amount of *cryptoassets* which form the *operational surplus* in any trust must not exceed a level that would be reasonably expected to be necessary, taking into account those services.

(5) The terms of the trust required under *CASS* 17.3.14R(2) and *CASS* 17.3.17R(3) must clearly set out that the *firm's* claim in the trust to the *operational surplus* in a particular *cryptoasset safeguarding class* is always and unconditionally subordinated to the claims of *clients* to *client cryptoassets* of that *cryptoasset safeguarding class* in the trust.

(6) When deciding to use a *operational surplus* in any trust that a *firm* operates under *CASS* 17.3.3R, the *firm* must make and retain a written record of the reason for the *operational surplus* to be necessary in order for the *firm* to provide services to one or more *clients* for whom the *firm* is *safeguarding cryptoassets* in the same trust (the '*per-trust operational surplus record*').

(7) The *firm* must not remove or reduce an *operational surplus* unless the amount removed represents an excess, and is removed following a *client cryptoasset reconciliation*, in accordance with *CASS* 17.5.12R.

17.3.21 R A *firm* must retain any *per-trust operational surplus record* made under *CASS* 17.3.20R(4) for a period of 5 years until after the *firm* ceases to use the *operational surplus* in that particular trust.

17.3.22 G (1) An example of where a *firm* may wish to use an operational surplus under *CASS* 17.3.20R(1) includes where the *firm's* service involves *qualifying cryptoasset staking* and, for example:

(a) it is necessary for the *firm* to contribute an amount of its own assets to meet the minimum threshold required by the staking protocol; or

(b) the staking rewards which are attributable to the *firm* (rather than any *client*) are received at a digital address pertaining to the trust.

(2) An example of where the exception at *CASS* 17.3.20R(3) may be relied on is to allow the *firm* to satisfy a requirement to pay transaction charges such as 'gas fees' in the *cryptoasset safeguarding class* that is required by the network when the transaction for which the *firm* is providing a service involves other *cryptoasset safeguarding classes*.

Guidance on trusts and appointing third parties

17.3.23 G (1) In cases where a *firm* appoints a third party to carry on the activity of *safeguarding cryptoassets* in accordance with *CASS* 17.6, the effect of *CASS* 17.3.3R and *CASS* 17.3.17R(1) means that the *firm's* contractual rights against that third party in relation to the relevant *client*

cryptoassets should be held on trust, because these are rights which can be exercised by virtue of the *firm safeguarding cryptoassets*.

(2) A *firm* in the position referred to in (1) should also comply with the other requirements of *CASS* 17.6.

17.4 Means of access

17.4.1 R This section applies to a *firm* when it is:

(1) *safeguarding cryptoassets* which are *client cryptoassets*; or

(2) *safeguarding cryptoassets* which would be *client cryptoassets* but are not being treated by the *firm* as *client cryptoassets* in reliance upon *CASS* 17.3.12R.

17.4.2 R The *rules* in this section apply where a *firm* undertakes any of the following activities in relation to the *means of access* to a *cryptoasset* in respect of which the *firm* is *safeguarding cryptoassets*:

(1) generating or creating the *means of access*, or any similar process;

(2) storing the *means of access*, in any form or medium of storage;

(3) exercising any form of control over the *means of access*;

(4) subjecting the *means of access* to any type of process; and

(5) destroying the *means of access*.

17.4.3 G (1) Because the *rules* in this section apply where a *firm* is *safeguarding cryptoassets*, this means that they do not apply where the *firm* does not have the requisite degree of 'control' as described at article 9N(4) of the *Regulated Activities Order*.

(2) The definition of *means of access* includes any means of which a *person* would need possession or knowledge to bring about a transfer of the benefit of a *cryptoasset* to another *person*.

(3) The scope of *CASS* 17.4.2R is broad and therefore the provisions in this section will apply to a range of activities and aspects of *safeguarding cryptoassets*, for example:

(a) using 'hot' or 'cold' devices or facilities to store the *means of access*;

(b) making and storing written records of the *means of access*; and

(c) processing the *means of access* by dividing a private cryptographic key into parts ('shards'), and (if relevant) distributing the shards amongst the *firm's* staff or other *persons* outside of the *firm*.

(4)

(a) If a *person* is, at a particular point in time, safeguarding only a single part of a private cryptographic key (eg, a 'shard') then, as a consequence of that fact by itself, they may be unlikely to have the requisite degree of 'control' as described at article 9N(4) of the *Regulated Activities Order* (assuming safeguarding just that one shard does not afford them the requisite degree of 'control' as described at article 9N(4)).

(b) However, if that *person* was previously in the position to create that shard and all the other shards from a private cryptographic key, then at that point they would have had the requisite degree of 'control' – even if after sharding the key they proceeded to distribute the other shards to other *persons*. Because they would have subjected the *means of access* to a process (the 'sharding' process), then as a result of *CASS* 17.4.2R(4) and the fact that they had the requisite degree of control at the time of the sharding, and assuming they are a *firm*, the requirements of this section would apply to that *firm*.

(c) Continuing from the example in (b) of a *firm* sharding a private cryptographic key and distributing it: if, after distributing the shards to other *persons* the *firm* can still require those other *persons* to return their shards under a binding agreement (or require their assistance to convene sufficient shards in order to digitally sign a transaction), then also as a result of *CASS* 17.4.2R(3), this section would apply to that *firm*.

(d) If any of the recipients of the shards had sufficient shards to themselves have the requisite degree of 'control' as described at article 9N(4) of the *Regulated Activities Order* then, assuming they are *firms*, as a result of *CASS* 17.4.2R(2), this section would apply to them also.

(5) In scenarios involving shards, the record required at *CASS* 17.4.8R(1)(d) should explain how the *firm* can exercise 'control', for example by setting out any relevant technical criteria which the *firm* is able to meet in order to digitally sign a transaction (such as a reconstruction or confirmation threshold), as well as how the *firm* is able to meet those criteria (for example, by a combination of retrieval from cold storage and requiring an appointed shard-holder to take certain steps).

17.4.4 R A *firm* must have robust security and organisational arrangements to ensure that, throughout the entire life cycle of any *means of access* to a *client cryptoasset*, the *means of access* are protected against the risks of inoperability, inaccessibility, loss, fraud and irrecoverability.

17.4.5 R A *firm* must promptly identify incidents of inoperability, inaccessibility, loss, fraud and irrecoverability to any *means of access* to a *client cryptoasset*.

17.4.6 R A *firm* must promptly resolve any incidents of inoperability, inaccessibility, loss, fraud and irrecoverability to any *means of access* to a *client cryptoasset*.

17.4.7 G In complying with *CASS* 17.4.4R to *CASS* 17.4.6R, a *firm* should, for example, consider whether, as relevant:

(1) its security and organisational arrangements adhere to any relevant international and industry standard practices;

(2) it is addressing any vulnerabilities to hacking and other risks of fraud and theft, including risks which originate from among the *firm's* own staff;

(3) it has a culture of detecting and acting on suspicious activity, including appropriate whistleblowing systems;

(4) it is addressing any:

(a) risks of 'single point of failure' (for example, as a result of a concentration of *means of access* with too few members of staff or on too few devices); and

(b) 'dependency risk' (for example as a result of distribution among too many members of staff or devices, or too much reliance on other *persons*);

(5) it has appropriate back-up and recovery systems;

(6) it has appropriate checks to ensure that the *means of access* remain accessible and operable, which themselves do not add undue security risks; and

(7) it employs random and non-deterministic methods as part of its security arrangements to minimise the risk of irreproducibility of any important data.

17.4.8 R (1) For each *means of access* that a *firm* controls at any particular point in time, and from the point at which the *firm* has such control, the *firm* must make and maintain a record which sets out the following information (the '*cryptoasset means of access record*'):

(a) the location (whether digital or physical) at which that *means of access* is being held including, where relevant, the virtual address for that *means of access*;

(b) a summary of the security measures which the *firm* has deployed for that *means of access* in accordance with *CASS*

17.4.4R, which must include the name of any other *persons* involved;

(c) the name of any natural *person*, such as a member of staff of the *firm*, who, to the *firm's* knowledge, is in a position to use that *means of access*;

(d) the way in which the *means of access*, whether by itself or in combination with other *means of access*, affords the *firm* 'control' over the relevant *cryptoasset* or *cryptoassets* in respect of which it is *safeguarding cryptoassets*; and

(e) whether the *means of access* has been destroyed (and, if so, when and the reason why it was destroyed).

(2) The *cryptoasset means of access record* under (1) must not contain or reproduce the *means of access* itself.

(3) The components of the *cryptoasset means of access record* under (1)(b) and (c) do not have to include the actual name of a *person* if doing so would compromise the *firm's* ability to comply with *CASS* 17.4.4R, provided that the record includes sufficient information from which the *person* can be identified using other records maintained by the *firm*.

17.4.9 R A *firm* must promptly update its *cryptoasset means of access records* required under *CASS* 17.4.8R as often as is necessary for the details within them to remain accurate.

17.4.10 R A *firm* must ensure that each *cryptoasset means of access record* is retained for a period of 5 years starting from whichever is the later of:

(1) the date it was created; or

(2) the date it was most recently modified.

17.4.11 R (1) A *firm* must create, retain and maintain a *means of access* policy document and a *means of access* procedures document which, taken together, explain the *firm's* means of complying with the requirements in *CASS* 17.4.4R to *CASS* 17.4.6R and *CASS* 17.4.8R to *CASS* 17.4.10R in clear and non-technical terms.

(2) A *firm* must review the documents under (1) at least once every year and make any necessary changes.

(3) A *firm* must retain each version of the documents required under (1) for a period of 5 years until after that version has been superseded by a new version.

17.5 Records of cryptoassets and reconciliations

17.5.1 R This section applies to a *firm* when it is *safeguarding cryptoassets* which are *client cryptoassets*.

General requirements

17.5.2 R A *firm* must keep such records as necessary to enable it at any time and without delay to distinguish *client cryptoassets* in respect of which the *firm* is *safeguarding cryptoassets* on behalf of one *client* from *client cryptoassets* in respect of which the *firm* is *safeguarding cryptoassets* on behalf of any other *client*, and from any *cryptoassets* which are not *client cryptoassets*.

17.5.3 R A *firm* must maintain its records in a way that ensures their accuracy, having regard to the business model of the *firm* and in particular the risks of:

(1) records becoming unreliable due to the nature of the *firm's* services and the networks relevant to the *client cryptoassets*; and

(2) the *firm* breaching the *rule* at *CASS* 17.3.3R.

17.5.4 R (1) A *firm* must establish and maintain systems and controls so that it can accurately determine the following and promptly identify and resolve any discrepancies in accordance with the *rules* in this section:

(a) for each trust that the *firm* has created under *CASS* 17.3.3R and in accordance with *CASS* 17.5.6R, the number of *client cryptoassets* of a particular *cryptoasset safeguarding class* in respect of which it is required to be *safeguarding cryptoassets* for a particular *client* (the *per-trust/client/class cryptoasset requirement*), taking into account its agreements with that *client* and any services that have been provided or are being provided to that *client*; and

(b) for each trust that the *firm* has created under *CASS* 17.3.3R and in accordance with *CASS* 17.5.7R, how many *client cryptoassets* of a particular *cryptoasset safeguarding class* it is *safeguarding cryptoassets* in relation to (the *per-trust/class cryptoasset resource*), whether itself or through the appointment of a third party under *CASS* 17.6.

(2) A *firm's* systems and controls under (1) must be designed to minimise the risks of inaccuracy, taking into account in particular:

(a) the time of day at which any processes to comply with *CASS* 17.5.6R to *CASS* 17.5.10R are run; and

(b) its arrangements for obtaining information from any third party appointed under *CASS* 17.6 in order to comply with *CASS* 17.5.7R.

(3) A *firm* must create, retain and maintain a reconciliations policy document and a reconciliations procedures document which, taken together, explain and set out:

(a) the *firm's* rationale for its procedures to comply with the *rules* in this section in clear and non-technical terms; and

(b) those procedures.

(4) A *firm* must review the documents under (3) at least once every year and make any necessary changes.

(5) A *firm* must retain each version of the documents required under (2) for a period of 5 years until after that version has been superseded by a new version.

17.5.5 G (1) Depending on the way a *firm* has complied with the *rules* in *CASS* 17.3, it may be necessary for the *firm*, when complying with the *rules* in this section, to make distinctions between different trusts that it has created under *CASS* 17.3.3R, and between different aspects of those trusts (such as whether or not it has decided for a particular trust to include an *operational surplus* under *CASS* 17.3.20R).

(2) When maintaining its records under the *rules* in this section, a *firm* should be making the distinctions referred to in (1) on the basis of its *client cryptoasset trust records*, which are required to be kept up to date under *CASS* 17.3.19R(2).

The per-trust/client/class cryptoasset requirement

17.5.6 R (1) A *firm* must calculate the *per-trust/client/class cryptoasset requirement* using the formula in (2) at least once each *business day*, with the result that, for each trust that the *firm* has created under *CASS* 17.3.3R, it produces, separately for each *client* that has an interest in that trust, the quantity of each *client cryptoasset* of each particular *cryptoasset safeguarding class* that the *firm* is required to hold for that *client* under that trust in accordance with the *rules* in *CASS* 17.3 (Cryptoasset safeguarding trusts).

(2) The *per-trust/client/class cryptoasset requirement* in (1) is calculated as (a) minus (b), where (a) and (b) are as follows:

(a) the sum of:

(i) the *firm's* previous *per-trust/client/class cryptoasset requirement* for the relevant trust, *client* and *cryptoasset safeguarding class*; and

(ii) the total of the following, each for the relevant trust:

(A) the number of *client cryptoassets* of the relevant *cryptoasset safeguarding class* which the *firm* has received from the *client* since the previous calculation;

(B) the number of *client cryptoassets* of the relevant *cryptoasset safeguarding class* which the *firm* has received on behalf of that *client* from any other *person* since the previous calculation;

(C) (to the extent not covered by (B)) the number of *client cryptoassets* of the relevant *cryptoasset safeguarding class* which have become due to the *client*, whether from the *firm* or earned in some other way, since the previous calculation; and

(D) (to the extent not covered by (B) or (C)) the number of *client cryptoassets* of the relevant *cryptoasset safeguarding class* which were required to be reinstated into the trust since the previous calculation under the *rules* at *CASS* 17.3 (Cryptoasset safeguarding trusts), including because of the end of a particular service; and

(b) the total of the following, each for the relevant trust:

(i) the number of *client cryptoassets* of the relevant *cryptoasset safeguarding class* which the *client* has withdrawn from the *firm* since the previous calculation;

(ii) the number of *client cryptoassets* of the relevant *cryptoasset safeguarding class* which the *firm* has transferred to another *person* on the *client's* instruction since the previous calculation;

(iii) the number of *client cryptoassets* of the relevant *cryptoasset safeguarding class* which have become due to the *firm* since the previous calculation, in respect of which the *firm* has a right to take ownership of the *cryptoasset* under *CASS* 17.3.10R;

(iv) the number of *client cryptoassets* of the relevant *cryptoasset safeguarding class* in respect of which the *firm* has relied on an exemption under *CASS* 17.3.4R, *CASS* 17.3.5R or *CASS* 17.3.6R to not hold the *cryptoassets* under the trust since the previous calculation;

(v) (to the extent not covered by (iii) or (iv)) the number of *client cryptoassets* of the relevant *cryptoasset*

safeguarding class which, since the previous calculation and as a result of services being provided by the *firm*, the *client* has been required to surrender; and

(vi) the number of *client cryptoassets* of the relevant *cryptoasset safeguarding class* in respect of which, following an unresolved shortfall, the *firm* has agreed with its *client* that it will no longer have to carry on *safeguarding cryptoassets*.

(3) A *firm* must use its internal records of *client* instructions, transactions and services to calculate any *per-trust/client/class cryptoasset requirement* under this *rule*, and must not use information from an external source (such as information contained on a blockchain or distributed ledger technology).

The per-trust/class cryptoasset resource

17.5.7 R (1) For each trust that a *firm* has created under *CASS* 17.3.3R, the *firm* must confirm the quantity of *client cryptoassets* of a particular *cryptoasset safeguarding class* in respect of which it is *safeguarding cryptoassets* under that trust at least once each *business day* (the '*per-trust/class cryptoasset resource*').

(2) The confirmation required under (1) must take account of both:

(a) the *client cryptoassets* of that particular *cryptoasset safeguarding class* which the *firm* can access in virtual addresses or devices; and

(b) where the *firm* has, under *CASS* 17.6, appointed a third party to carry on the activity of *safeguarding cryptoassets*, the *client cryptoassets* for which either:

(i) the third party has confirmed to the *firm* that it has the *means of access* to itself; or

(ii) in cases where that third party has appointed a further third party with the *firm's* consent under *CASS* 17.6.9R, the third party appointed by the *firm* has confirmed to the *firm* that the further third party has the *means of access* to.

(3) A *firm* must use external sources of information to confirm any *per-trust/class cryptoasset resource* under this *rule*, and must not use any internal source of information which the *firm* uses to calculate any *per-trust/client/class cryptoasset requirement* under *CASS* 17.5.6R

17.5.8 G (1) The requirements at *CASS* 17.5.6R(3) and at *CASS* 17.5.7R(3) are to ensure that a *firm's client cryptoasset reconciliations* use independent sources of information, with the effect that the *client cryptoasset*

reconciliations will be effective in their purpose of identifying discrepancies.

(2) A *firm* may use information from an external source such as information contained on the appropriate distributed ledger technology network to confirm the information described at *CASS* 17.5.7R(2)(a).

(3) Although information contained on a blockchain or distributed ledger technology may give an indication as to the information described at *CASS* 17.5.7R(2)(b), a *firm* should only use information provided from a third party appointed under *CASS* 17.6 in order to confirm that information.

(4) The requirements at *CASS* 17.5.6R(3) and at *CASS* 17.5.7R(3) should not prevent a *firm* from investigating and resolving any discrepancy under *CASS* 17.5.10R(3) or *CASS* 17.5.11R(1).

(5) When a *firm* is ascertaining the quantity for the *per-trust/class cryptoasset resource* under *CASS* 17.5.7R, it should not make any adjustment or allowance for *cryptoassets* in the relevant trust environment that may be part of an *operational surplus* which the *firm* has decided to include under *CASS* 17.3.20R.

17.5.9 R (1) Each time a *firm* calculates a *per-trust/client/class cryptoasset requirement* or confirms a *per-trust/class cryptoasset resource*, it must make a record of:

(a) the date and time it carried out that calculation or confirmation, as appropriate;

(b) the actions it took in order to carry out that calculation or confirmation, as appropriate; and

(c) the calculation result or confirmation outcome, as appropriate.

(2) A *firm* must retain each record made under (1) for a period of 5 years.

Client cryptoasset reconciliations

17.5.10 R (1) For each trust that a *firm* has created under *CASS* 17.3.3R, a *firm* must perform a *client cryptoasset reconciliation* under this *rule* at least once each *business day*, to check whether it has breached the *rules* in *CASS* 17.3 to hold *client cryptoassets* on trust.

(2) For each *cryptoasset safeguarding class* in respect of which the *firm* is required to be *safeguarding cryptoassets* within the relevant trust, the *firm* must compare the total of the *per-trust/client/class cryptoasset requirements* for all *clients* who have an interest in that trust with the *per-trust/class cryptoasset resource* for that trust at the same point in time.

(3) If the *firm* identifies a discrepancy as a result of carrying out a *client cryptoasset reconciliation*, it must promptly investigate the reason for the discrepancy and resolve it without delay or, where there is a shortfall, in accordance with *CASS* 17.5.13R.

(4) Each time a *firm* performs a *client cryptoasset reconciliation*, it must make a record (a '*client cryptoasset reconciliation record*') of:

(a) the date and time of the *client cryptoasset reconciliation*;

(b) whether or not the *client cryptoasset reconciliation* identified any discrepancies and, if so:

(i) the extent of them; and

(ii) the reasons for them; and

(c) any actions taken or attempted by the *firm* in relation to those discrepancies, including under *CASS* 17.5.12R and *CASS* 17.5.13R.

(5) A *firm* must retain each *client cryptoasset reconciliation record* made under (4) for a period of 5 years.

Other discrepancies

17.5.11 R (1) If a *firm* identifies a discrepancy related to its *safeguarding* of *client cryptoassets* outside of its processes for a *client cryptoasset reconciliation*, it must promptly investigate the reason for the discrepancy and resolve it without delay or, where there is a shortfall, in accordance with *CASS* 17.5.13R.

(2) Each time a *firm* identifies a discrepancy under (1), it must make a record (a '*client cryptoasset discrepancy record*') of:

(a) the date and time the discrepancy was identified;

(b) the reasons for the discrepancy and the extent of it; and

(c) any actions taken or attempted by the *firm* in relation to the discrepancy, including under *CASS* 17.5.12R and *CASS* 17.5.13R.

(3) A *firm* must retain each *client cryptoasset discrepancy record* made under (2) for a period of 5 years.

Client cryptoasset reconciliation excesses

17.5.12 R (1) This *rule* applies where a *firm's client cryptoasset reconciliation* for a particular trust shows that the *firm*, having investigated any discrepancies under *CASS* 17.5.10R(3) or *CASS* 17.5.11R(1), has confirmed there to be a greater amount of *cryptoassets* within that trust

for a particular *cryptoasset safeguarding class* than the total of the *per-trust/client/class cryptoasset requirements* for all *clients* who have an interest in that trust for that *cryptoasset safeguarding class*.

(2) Subject to (3), the *firm* must, before its next *client cryptoasset reconciliation* for that trust, remove all the excess *cryptoassets* of that particular *cryptoasset safeguarding class* from that trust.

(3) The *firm* may only retain excess *cryptoassets* of that particular *cryptoasset safeguarding class* within that trust if:

(a) it had previously decided to use an *operational surplus* in that trust and in that *cryptoasset safeguarding class* of *cryptoasset* in accordance with *CASS* 17.3.20R;

(b) the *firm's* retention of the excess does not cause the *firm* to be in breach of *CASS* 17.3.20R(2) or (3); and

(c) the amount of any excess that is withdrawn under this *rule*, and the amount of any excess that is retained under this *rule*, are recorded in the relevant *client cryptoasset reconciliation record* under *CASS* 17.5.10R(4)(c) or the relevant *client cryptoasset discrepancy record* under *CASS* 17.5.11R(2)(c), as appropriate.

Client cryptoasset reconciliation shortfalls

17.5.13 R (1) This *rule* applies where a *firm's client cryptoasset reconciliation* for a particular trust identifies a discrepancy as a result of, or that reveals, a shortfall which the *firm* has not yet resolved.

(2) A shortfall for the purposes of this *rule* is a situation for a particular trust under *CASS* 17.3.3R in which the *firm's per-trust/class cryptoasset resource* shows that there is a lesser amount of *cryptoassets* within that trust for a particular *cryptoasset safeguarding class* than the total of the *per-trust/client/class cryptoasset requirements* for all *clients* who have an interest in that trust in relation to that *cryptoasset safeguarding class*.

(3) This *rule* also applies where, outside of its processes for *client cryptoasset reconciliations*, a *firm* identifies a discrepancy as a result of, or that reveals, a shortfall which the *firm* has not yet resolved.

(4) The *firm* must address the shortfall by ensuring that, no later than 24 hours after identifying the discrepancy, the *firm* has the correct number of *client cryptoassets* on trust.

(5) Where necessary to comply with the requirement at (4), the *firm* must:

(a) appropriate its own *cryptoassets* in the relevant *cryptoasset safeguarding class*;

(b) acquire *cryptoassets* in the relevant *cryptoasset safeguarding class* using its own resources; or

(c) procure a third party appointed under *CASS* 17.6 to apply or acquire its own *cryptoassets* in the relevant *cryptoasset safeguarding class* to resolve the shortfall.

(6) Each measure taken by a *firm* to comply with (4) must be recorded in the relevant *client cryptoasset reconciliation record* under *CASS* 17.5.10R(4)(c) or the *relevant client cryptoasset discrepancy record* under *CASS* 17.5.11R(2)(c), as appropriate.

(7) A shortfall will not be considered to be addressed under (4) if *cryptoassets* of another *cryptoasset safeguarding class*, or some other type of asset (e.g. *money*), are placed in the trust.

17.5.14 G (1) *CASS* 17.5.13R does not prevent a *firm* from setting aside an alternative asset for the relevant *client(s)*, or paying/transferring an alternative asset to them, in an amount which would match any claim that they might have against the *firm* for the shortfall – for example, where doing so is required under the *firm's* agreement with the *client(s)*, is required by the *FCA*, or is considered by the *firm* to be required for another reason.

(2) Where a *firm* takes the action described in (1) involving an alternative asset, this does not have the automatic consequence that the *firm* will have addressed the shortfall as required under *CASS* 17.5.13R(4).

(3) However, it may put the *firm* and *client* in a position to agree that the *firm* need no longer carry on the activity of *safeguarding cryptoassets* in relation to the *cryptoassets* in shortfall, which may then be reflected in the *per-trust/client/class cryptoasset requirement* (see *CASS* 17.5.6R(2)(b)(vi)).

(4) In making any such agreement with a *client* in the course of *retail market business*, whether in advance or at the time of the shortfall, a *firm* should act compatibly with its obligations under the *Consumer Duty*.

17.5.15 R Where a *firm* fails to address a shortfall as required by *CASS* 17.5.13R, it must immediately:

(1) notify each affected *client* in writing (including those who are affected because they have an interest in the relevant trust which has, under the terms of that trust, reduced); and

(2) notify the *FCA* in writing, setting out:

(a) the reasons for the shortfall and the reasons for the *firm* failing to address it;

(b) the name of each *cryptoasset safeguarding class* of *cryptoasset* for which there is a shortfall, identified using the name of the *cryptoasset* or an identification code, in either case from which the relevant *cryptoasset safeguarding class* can be precisely distinguished, and the amount of that shortfall in that *cryptoasset safeguarding class*;

(c) the number of *clients* in the relevant trust affected by the shortfall and by how much each affected *client* is affected;

(d) the *firm's* expected timeframe for resolution of the shortfall, including detail on the steps which the *firm* and any third parties intend to follow to achieve resolution; and

(e) the approach the *firm* is taking in relation to *client* notifications under (1).

Other notification requirements

17.5.16 R A *firm* must notify the *FCA* in writing without delay if either of the following apply:

(1) its internal records relating to *safeguarding cryptoassets* are materially out of date, or materially inaccurate or invalid; or

(2) it will be unable, or materially fails, to comply with *CASS* 17.5.6R, *CASS* 17.5.7R or *CASS* 17.5.10R.

17.6 Appointing third parties to safeguard cryptoassets

17.6.1 R This section applies to a *firm* when it *safeguards cryptoassets* which are *client cryptoassets* and, in the course of carrying on that activity, it *arranges cryptoasset safeguarding*.

Purpose of this section

17.6.2 G (1) Where a *firm* carries on the activity of *safeguarding cryptoassets*, it may be necessary for the *firm* to appoint a third party to carry on the activity of *safeguarding cryptoassets* under the *firm's* direction in relation to a particular *client cryptoasset* or *client cryptoassets* of one or more *cryptoasset safeguarding classses*.

(2) That third party appointed by the *firm* may itself be a *firm* or may, for example, be a *person* who is *overseas* and who is not required to be *authorised* to carry on the activity of *safeguarding cryptoassets* in these circumstances.

(3) This section sets out the *rules* that apply to such an appointment by a *firm* of a third party to carry on that activity in order to address the risk of harm to the *firm's clients* that might result from that appointment, particularly in cases where the third party is not itself *authorised*.

(4) In the *FCA's* view, where a *firm* appoints a third party to carry on the activity of *safeguarding cryptoassets* in relation to any *client cryptoasset*, the *firm* will be carrying on the activities of both *safeguarding cryptoassets* and *arranging cryptoasset safeguarding*. In that situation, the *firm*, while remaining a trustee who is *safeguarding cryptoassets*, arranges for another *person* to *safeguard cryptoassets* under the *firm's* direction.

(5) The scenario described in (4) is different to one in which a *firm* only carries on *arranging cryptoasset safeguarding* and does not itself carry on *safeguarding cryptoassets*. In that situation, in making the arrangements which will result in the *client* receiving the service of *safeguarding cryptoassets* from another *person*, the *firm* is not itself a trustee of the *cryptoassets*.

(6) This section would not apply to the scenario described in (5) in which a *firm* only carries on *arranging cryptoasset safeguarding*. The *rules* in *CASS* 17.7 apply to a *firm* that only carries on *arranging cryptoasset safeguarding*.

(7) This section would not apply where the *firm* appoints a third party to hold part of a *means of access* where the third party would not be *safeguarding cryptoassets* because it lacks the requisite degree of 'control'. An example of this is where the *firm* appoints a third party to hold a shard of a private cryptographic key, but possession or knowledge of that shard, by itself, would not put the third party in a position to be able to transfer the benefit of the relevant *client cryptoasset*.

The conditions for appointing third parties to safeguard cryptoassets

17.6.3 R (1) A *firm* may appoint and retain another *person* (a 'third party') to carry on the activity of *safeguarding cryptoassets* in respect of which the *firm* has undertaken to its *client* to carry on *safeguarding cryptoassets*, but only if the following conditions are met:

(a) the third party operates in a jurisdiction which specifically regulates the safeguarding of *cryptoassets* through mandatory requirements concerning financial and operational resilience, security of the *means of access* to *cryptoassets*, and record-keeping, and the activities of the third party pursuant to the appointment by the *firm* are supervised in that jurisdiction;

(b) the *firm* has concluded, having completed the due diligence and any periodic review required under *CASS* 17.6.5R, that the appointment of the third party would not increase the risk of loss or diminution of any *client cryptoassets* which are subject to the arrangement, having regard to the *firm's* compliance with *CASS* 17.2.2R;

(c) in relation to a *firm's retail market business*, the appointment of the third party is compatible with the *Consumer Duty*;

(d) prior to the appointment commencing, the *firm* has entered into an agreement with the third party in the form required at *CASS* 17.6.6R; and

(e) the *firm* has met the governance requirements at *CASS* 17.6.9R.

(2) A contravention of (1)(c) does not give rise to a right of action by a private person under section 138D of the *Act* (and *CASS* 17.6.3R(1)(c) is specified under section 138D(3) of the *Act* as a provision giving rise to no such right of action).

(3) A contravention of any other aspect of this *rule* is not affected by (2).

17.6.4 G (1) Where a *client* has instructed a *firm* to appoint a particular third party, the *firm* should still ensure that the conditions for the appointment at *CASS* 17.6.3R are met.

(2) To meet the condition at *CASS* 17.6.3R(1)(a) it is not essential that the mandatory requirements of the other jurisdiction refer to the specific terms mentioned in that requirement (e.g. 'financial and operational resilience', 'security of the *means of access* to *cryptoassets*', and 'record-keeping') provided that they focus on all of those aspects in substance.

Mandatory due diligence

17.6.5 R (1) A *firm* must exercise all due skill, care and diligence in the selection, appointment and periodic review of the third party and of the arrangements for the *safeguarding* of the relevant *client cryptoassets*, in order to conclude that the appointment of the third party would not increase the risk of loss or diminution of any *client cryptoassets* which are subject to the arrangement.

(2) When a *firm* makes the selection and appointment and conducts the periodic review referred to under this *rule*, it must take into account:

(a) whether the third party has the appropriate regulatory permissions to carry out the appointment;

(b) the arrangements that the third party has in place for *safeguarding cryptoassets*;

(c) the capacity and capability of the third party to provide the contracted services;

(d) the capital or financial resources of the third party;

(e) the creditworthiness of the third party;

(f) the potential impact on the contracted services of any other activities undertaken by the third party and, if relevant, any *affiliated company*;

(g) the expertise and market reputation of the third party;

(h) any legal requirements relating to the carrying on of *safeguarding cryptoassets* in respect of the relevant *cryptoassets* that could adversely affect the *firm's clients'* rights;

(i) market practices relating to the carrying on of *safeguarding cryptoassets* in respect of the *cryptoassets* that could adversely affect the *firm's clients'* rights;

(j) any relevant industry standard reports, including in relation to security; and

(k) where the third party appointed by the *firm* has appointed a further third party with the *firm's* consent under *CASS* 17.6.9R, all the factors set out above in relation to that further third party.

(3) The *firm* must conduct the periodic review required under this *rule* at least once each year.

The agreement condition

17.6.6 R A *firm* must have entered into a written agreement with any third party that it appoints to carry on the activity of *safeguarding cryptoassets* under *CASS* 17.6.3R. This agreement must, at minimum:

(1) set out the binding terms of the arrangement between the *firm* and the third party;

(2) be in force for the duration of the appointment;

(3) clearly set out the service(s) that the third party is contracted to provide;

(4) require the third party to seek and obtain the *firm's* written consent prior to the third party being able to appoint a further, different third party to carry on the activity of *safeguarding cryptoassets*;

(5) in recognition that the *firm* is acting as a trustee in relation to the *client cryptoassets* that are subject to the appointment:

(a) require that any *client cryptoassets* that are subject to the appointment are not co-mingled with, and are identifiable separately from, any assets belonging to the third party;

(b) require that any *client cryptoassets* that are subject to the appointment are not co-mingled with, and are identifiable separately from, any assets belonging to the *firm* for which it is not acting as a trustee;

(c) require that any *client cryptoassets* that are subject to the appointment are not co-mingled with, and are identifiable separately from, any assets pertaining to any other appointment;

(d) require the third party to recognise that the *firm* acts for its *clients* as trustee over the *client cryptoassets*; and

(e) exclude any rights of the third party to exercise set-off or counterclaim against the *client cryptoassets* in respect of any debt owed to it or to any other *person*;

(6) require the third party to notify the *firm* whenever *cryptoassets* are no longer subject to the terms of the agreement for any reason;

(7) include provisions detailing the extent of the third party's liability in the event of the loss of a *client cryptoasset* caused by the fraud, wilful default or negligence of the third party or an agent appointed by the third party; and

(8) set out the procedures and authorities for the passing of instructions to, or by, the *firm*.

17.6.7 R A *firm* must take the necessary steps to ensure that both it and the third party adhere to the agreement referred to at *CASS* 17.6.6R at all times.

Consenting to safeguarding chains

17.6.8 R (1) This *rule* applies where, under the mandatory term described at *CASS* 17.6.6R(4), a third party appointed by the *firm* seeks the *firm's* consent to itself appoint a further, different third party to carry on the activity of *safeguarding cryptoassets* in relation to *client cryptoassets* which the *firm* has undertaken to its *client* to *safeguard*.

(2) The *firm* must withhold the consent referred to in (1) unless it is satisfied that:

(a) the further appointee operates in a jurisdiction which specifically regulates the safeguarding of *cryptoassets* through mandatory requirements concerning financial and operational resilience, security of the *means of access* to *cryptoassets*, and record-keeping, and the activities of the further appointee are supervised in that jurisdiction;

(b) the *firm* has concluded, having completed due diligence on the further appointee in line with the requirements under *CASS* 17.6.5R, that the further appointment would not increase the

risk of loss or diminution of any *client cryptoassets* which are subject to the arrangement, having regard to the *firm's* compliance with *CASS* 17.2.2R;

(c) in relation to a *firm's retail market business*, the further appointment is compatible with the *Consumer Duty*; and

(d) the agreement under which the further appointment will be governed (as between the third party appointed directly by the *firm* and the further third party) contains terms which provide equivalent safeguards to those set out at *CASS* 17.6.6R(1) to (8).

(3) (a) The *firm* may approach its assessment under (2)(b) by requiring the third party it has appointed under *CASS* 17.6.3R to apply the factors set out at *CASS* 17.6.5R(2) in relation to the further appointee and to report its conclusions to the *firm*.

(b) Where a *firm* takes the approach in (a), it remains fully responsible for complying with the *rules* in this section in relation to the further appointment.

(4) Any consent given by the *firm* under this *rule* must be periodically reviewed, at least once each year.

(5) A contravention of (2)(c) does not give rise to a right of action by a private person under section 138D of the *Act* (and *CASS* 17.6.8R(2)(c) is specified under section 138D(3) of the *Act* as a provision giving rise to no such right of action).

(6) A contravention of any other aspect of this *rule* is not affected by (5).

The governance condition

17.6.9 R (1) Each proposed appointment by the *firm* of a third party under *CASS* 17.6.3R and each proposed consent under *CASS* 17.6.8R, together with the *firm's* considerations and conclusions to support that proposal, must be approved by the *firm's governing body* before the appointment is made or the consent is given, or by a *person* or *persons* within the *firm* to whom the *firm's governing body* has delegated that role (the '*governing body's* delegate').

(2) Where the *governing body* has delegated one or more *persons* for the purposes of the approval under (1), that delegation must include the *SMF manager* to whom the *firm* has appointed the *FCA-prescribed senior management responsibility* (Reference letter (z)) in the table in *SYSC* 24.2.6R (functions in relation to *CASS*).

(3) The outcome of each periodic review of a *firm's* selection and appointment of a third party that it conducts under *CASS* 17.6.5R, together with the *firm's* considerations and conclusions, must be

approved by the *firm's governing body* or the *governing body's* delegate within 3 *months* of the review being concluded.

Policy on appointing third parties

17.6.10 R (1) A *firm* must produce and maintain a written policy that sets out its methodology for any selections, appointments, periodic reviews and consents that are required under *CASS* 17.6.3R, *CASS* 17.6.5R and *CASS* 17.6.8R.

(2) A *firm* must retain the written policy under (1) until 5 years after it has been superseded by any new version of the written policy, or otherwise indefinitely.

Records

17.6.11 R (1) A *firm* must make a record of how the requirements of *CASS* 17.6.3R(1) or *CASS* 17.6.8R(2) are met in relation to any appointment of a third party under *CASS* 17.6.3R or consent to a further appointment of a third party under *CASS* 17.6.8R. That record must include the conclusions of any due diligence exercise carried out in accordance with those *rules*, making explicit reference to the factors set out at *CASS* 17.6.5R(2)(a) to *CASS* 17.6.5R(2)(j) (a '*client cryptoasset third party due diligence record*').

(2) A *firm* must make the record under (1) prior to the relevant appointment commencing or the relevant consent being given.

(3) Whenever a *firm* undertakes a periodic review of its selection and appointment of a third party under *CASS* 17.6.5R or of the *firm's* consent to an appointment under *CASS* 17.6.8R(4), the *firm* must make a record of the conclusions of its review, making explicit reference to the factors set out at *CASS* 17.6.5R(2)(a) to *CASS* 17.6.5R(2)(j) (a '*client cryptoasset third party review record*').

(4) A *firm* must make the record under (3) on the date it completes the review.

(5) A *firm* must make a record of each approval given by its *governing body* or its *governing body's* delegate under *CASS* 17.6.9R(1) or (3) (a '*client cryptoasset third party governance record*').

(6) A *firm* must make the record under (5) on the date of the *governing body's* or its *governing body's* delegate's approval.

(7) A *firm* must retain the records under (1), (3) and (5) until 5 years after the relevant appointment ceases.

17.7 Arranging cryptoasset safeguarding

17.7.1 R This section applies to a *firm* when it *arranges cryptoasset safeguarding*, but is not *safeguarding cryptoassets* in relation to which it is *arranging cryptoasset safeguarding*.

Agreements

17.7.2 R Each time a *firm*, on behalf of a *client*, *arranges cryptoasset safeguarding* with another *person*, it must enter into an agreement with that other *person*. This agreement must, at minimum:

(1) set out the obligations between the *firm* and the other *person*, including any ongoing obligations of the *firm*;

(2) set out the basis for any payments or other consideration between the two parties; and

(3) include provisions detailing the extent of either party's liability in the event of the loss of a *cryptoasset*.

Records

17.7.3 R (1) When a *firm arranges cryptoasset safeguarding*, it must ensure that proper records of the arrangements are made at the time the arrangements are put in place, and at the time the arrangements are amended (a '*cryptoasset safeguarding arrangement record*').

(2) A *firm* must retain the records made under (1) for a period of 5 years after they are made.

Amend the following as shown.

Sch 1 Record keeping requirements

…

Sch 1.3 G

Handbook reference	Subject of record	Contents of record	When record must be made	Retention period
…				
CASS 16.7.10R	…	…	…	…
CASS 17.3.6R(3)	*Client cryptoasset trust exemption record*	A record of a *firm's* reasons for concluding that it is necessary for the exemption at	Prior to providing the relevant service to any *client*	5 years after it has stopped providing the relevant service

		CASS 17.3.6R(1) to be used to provide a service		
CASS 17.3.11R(4)	*Client cryptoasset trust exemption consent record*	A record of a *firm's client's* written consent under *CASS* 17.3.5R(4) or *CASS* 17.3.6R(1)(c) for the *firm* to use the exemption at *CASS* 17.3.5R(1) or *CASS* 17.3.6R(1) respectively	Prior to making use of the exemption in relation to the *client's client cryptoasset*	5 years after it has stopped relying on the consent to use the exemption at *CASS* 17.3.5R(1) or *CASS* 17.3.6R(1)
CASS 17.3.16R	The document required under *CASS* 17.3.14R(2) setting out the terms of a trust (e.g. a deed)	The terms of the trust and details of any amendments which were made to the terms after the trust was first created	At the time the trust is created	5 years after the trust has been brought to an end
CASS 17.3.19R	*Client cryptoasset trust record*	Details of a trust that a *firm* has created under *CASS* 17.3.3R	At the time the *firm* creates the trust to which the *client cryptoasset trust record* pertains	5 years after the relevant trust has been brought to an end
CASS 17.3.21R	*Per-trust operational surplus record*	The reason for it being necessary for the *firm* to use an *operational surplus* for a particular trust created under *CASS* 17.3.3R	When the *firm* decides to use an *operational surplus* in a trust that the *firm* operates under *CASS* 17.3.3R	5 years until after the *firm* ceases to use the *operational surplus* in that particular trust
CASS 17.4.8R	*Cryptoasset means of access record*	Details of each *means of access* that the *firm* controls	When the *firm* starts to control the *means of access*	5 years after the later of the date the record was created and the date it was most

				recently modified
CASS 17.4.11R	Each version of a *firm's means of access* policy document and *means of access* procedures document	An explanation of the *firm's* means of complying with the requirements in *CASS* 17.4.4R to *CASS* 17.4.6R and *CASS* 17.4.8R to *CASS* 17.4.10R in clear and non-technical terms	Not specified	5 years after the version has been superseded by a new version
CASS 17.5.4R(3)	Each version of a *firm's* reconciliations policy document and reconciliations procedures document	The *firm's* rationale for its procedures to comply with the *rules* in *CASS* 17.5 in clear and non-technical terms, and those procedures	Not specified	5 years after the version has been superseded by a new version
CASS 17.5.9R	The *firm's per-trust/client/class cryptoasset requirement* and *per-trust/class cryptoasset resource*	The date and time, the actions taken and the outcome	Whenever the *firm* calculates a *per-trust/client/class cryptoasset requirement* or confirms a *per-trust/class cryptoasset resource*	5 years
CASS 17.5.10R(4)	*Client cryptoasset reconciliation record*	The date and time, whether there were any discrepancies and the reasons for them, and any actions taken	Each time a *firm* performs a *client cryptoasset reconciliation*	5 years
CASS 17.5.11R(2)	*Client cryptoasset discrepancy record*	The date and time, the reasons for the discrepancy and any actions taken	Each time a *firm* identifies a discrepancy outside of its processes for a	5 years

			client cryptoasset reconciliation	
CASS 17.6.10R	Each version of a *firm's* policy for the appointment of third parties under *CASS* 17.6	The *firm's* methodology for any selections, appointments, periodic reviews and consents that are required to be carried out under *CASS* 17.6.3R, *CASS* 17.6.5R and *CASS* 17.6.8R	Not specified	5 years after the version has been superseded by a new version
CASS 17.6.11R(1)	*Client cryptoasset third party due diligence record*	The grounds upon which the *firm's governing body* was satisfied of meeting the requirements of *CASS* 17.6.3R(1) to (4) or *CASS* 17.6.8R	Prior to the relevant appointment commencing	5 years after the relevant appointment ceases
CASS 17.6.11R(3)	*Client cryptoasset third party review record*	The conclusions of any periodic review performed under *CASS* 17.6.5R	The date the *firm* completes the review	5 years after the relevant appointment ceases
CASS 17.6.11R(5)	*Client cryptoasset third party governance record*	A *firm's governing body's* or its *governing body's* delegate's approval under *CASS* 17.6.9R(3)	The date of the *governing body's* or the *governing body's* delegate's approval	5 years after the relevant appointment ceases
CASS 17.7.3R(1)	*Cryptoasset safeguarding arrangement record*	A record of *arranging cryptoasset safeguarding*	When the *firm arranges cryptoasset safeguarding*	5 years

Sch 2 Notification requirements

Sch 2.1 G

Handbook reference	Matter to be notified	Contents of notification	Trigger event	Time allowed
…				
CASS 16.6.9R(3)(b)	…	…	…	…
CASS 17.5.15R	Failure to address a shortfall as required by *CASS* 7.5.13R	The reasons and other details as set out at *CASS* 17.5.15R(2)	Failure to address a shortfall	Immediately
CASS 17.5.16R(1)	The *firm's* internal records relating to *safeguarding cryptoassets* being materially out of date, or materially inaccurate or invalid	The fact of this issue	The *firm's* internal records relating to *safeguarding cryptoassets* being materially out of date, or materially inaccurate or invalid	Without delay
CASS 17.5.16R(2)	The *firm* being unable, or materially failing, to comply with *CASS* 17.5.6R, *CASS* 17.5.7R or *CASS* 17.5.10R	The fact of this issue	The *firm* being unable, or materially failing, to comply with *CASS* 17.5.6R, *CASS* 17.5.7R or *CASS* 17.5.10R	Without delay

…

Sch 5 Rights of actions for damages

…

Sch 5.2 G

		Paragraph	Right of action under Section 138D

Chapter / Appendix	Section / Annex		For private person?	Removed?	For other person?	
All *rules* in *CASS* with the status letter "E"			No	No	No	
All other *rules* in *CASS*, except *CASS* 6.4.1BAR(2)(c) ~~and~~, *CASS* 7.11.32R(2), *CASS* 17.1.6R(1), *CASS* 17.3.11R(2), *CASS* 17.6.3R(1)(c) and *CASS* 17.6.8R(2)(c).			Yes	No (except under *CASS* 6.4.1BBR ~~and~~, *CASS* 7.11.32AR, *CASS* 17.1.6R(2), *CASS* 17.3.11R(6), *CASS* 17.6.3R(2) and *CASS* 17.6.8R(5))	No	

12 Endeavour Square London E20 1JN
Telephone: +44 (0)20 7066 1000
Website: www.fca.org.uk

Pub ref: 2-008542.2

All our publications are available to download from www.fca.org.uk.

Request an alternative format

Please complete this form if you require this content in an alternative format.

Or call 0207 066 1000

Sign up for our **news and publications alerts**