

Discussion Paper **DP24/4**

Regulating cryptoassets: Admissions & Disclosures and Market Abuse Regime for Cryptoassets

December 2024

How to respond

We are asking for comments on this Discussion Paper (DP) by **14 March 2025**.

You can send them to us using the form on our [website](#).

Or in writing to:

Wholesale Cryptoasset
Policy
Financial Conduct Authority
12 Endeavour Square
London E20 1JN

Email:

dp24-4@fca.org.uk

Disclaimer

We make all responses to formal consultations available for public inspection unless the respondent requests otherwise. We will not regard a standard confidentiality statement in an email message as a request for non-disclosure.

Despite this, we may be asked to disclose a confidential response under the Freedom of Information Act 2000. We may consult you if we receive such a request. Any decision we make not to disclose the response is reviewable by the Information Commissioner and the Information Rights Tribunal.

Further information on the FCA's use of personal data can be found on the FCA website at: www.fca.org.uk/privacy.



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

See all our latest press releases, consultations and speeches.

Contents

Chapter 1	Overview	Page 4
Chapter 2	Admissions and disclosures	Page 14
Chapter 3	Market abuse	Page 28
Chapter 4	Conclusion	Page 51
Annex 1	List of questions	Page 52
Annex 2	Glossary	Page 58
Annex 3	Abbreviations used in this paper	Page 60

Chapter 1

Overview

Introduction

- 1.1** In 2023, the government announced plans to legislate for a future financial services regime for cryptoassets. This would bring certain cryptoasset activities into the FCA's regulatory perimeter. The Treasury published its initial consultation and call for evidence in February 2023, followed by its response in October.
- 1.2** In November 2024, the new government confirmed it will proceed with legislation to bring cryptoassets into the FCA's regulatory perimeter. The approach will closely align with the proposals set out in the previous government's consultation, with one key difference: the government will no longer pursue a 'phased approach' towards crypto legislation. This means that fiat-referenced stablecoin activities (previously 'phase 1') will be legislated for at the same time as crypto trading, exchange, and other activities (previously 'phase 2').
- 1.3** In June 2023, the law was changed and included a broad definition of cryptoassets as 'any cryptographically secured digital representation of value or contractual rights that –
- a.** can be transferred, stored or traded electronically, and
 - b.** that uses technology supporting the recording or storage of data (which may include distributed ledger technology)'.
- 1.4** As discussed in the consultation response, the government intends to narrow this scope through secondary legislation where appropriate for the purposes of specific regulatory regimes.
- 1.5** 'Cryptoassets' in this paper refers to spot cryptoassets, such as stablecoins and unbacked cryptoassets (for example, Bitcoin and Ether). It does not include those already captured under the existing list of 'specified investments' in Part III of the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (RAO), such as tokenised financial instruments, or the rights to the same, which includes security tokens.
- 1.6** Under the government's plans, our regulatory remit for cryptoassets will expand from the current Money Laundering, Terrorist Financing, and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs) and Financial Promotions regime to a more comprehensive conduct regime. This will cover cryptoasset trading, regulation of stablecoins, intermediation, custody, and other core activities.
- 1.7** Our focus in this Discussion Paper (DP) is on the future market abuse regime for cryptoassets (MARC) and cryptoasset admissions and disclosures regime (A&D). We want this DP to help inform the development of a balanced regime that addresses market risks without stifling growth.

Figure 1. FCA Crypto Roadmap

This outlines planned FCA policy publications for cryptoassets where we are seeking feedback and the content they are expected to cover.

Not exhaustive; all timelines are subject to change according to parliamentary time and/or further steers from government



Financial Promotions
rules go live

Stablecoins
issuance and custody

DP

Current stage



Trading platform rules including location, access, matching and transparency requirements

Intermediation rules including order handling and execution requirements

Lending rules including ownership, access and disclosures

Staking rules including ownership and disclosures

Prudential considerations for cryptoasset exposures

DP

Conduct and firm standards for all Regulated Activities Order (RAO) activities

Systems and controls including Operational Resilience and Financial Crime

Consumer Duty

Complaints

Conduct (COBS)

Governance including Senior Managers and Certification Regime (SMCR)

CP

Final rules

All Policy Statements published

PS

Regime go-live

Q1 2020

Q4 2023

Money Laundering Regulations
legislation applies

DP

Admission and disclosures

Admission/rejection processes

Disclosures

Liability

Due diligence

National Storage Mechanism (NSM)

Market abuse

Systems and controls

Information sharing

Inside information disclosure

Q1/Q2 2025

CP

Stablecoins

Backing assets

Redemption

Custody

Recordkeeping

Reconciliations

Segregation of assets

Use of 3rd parties

Prudential

Introduction of a new prudential sourcebook, including capital, liquidity and risk management

Q3 2025

CP

Admissions and Disclosures

As per DP

Market Abuse

As per DP

Q4 2025/
Q1 2026

CP

Trading platforms, intermediation, lending and staking

As per DP +

Resolution

Remaining material for prudential sourcebook

Groups

Reporting

2026

Gateway readiness

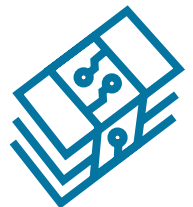
Gateway opens

Key

DP Discussion Paper/s

CP Consultation Paper/s

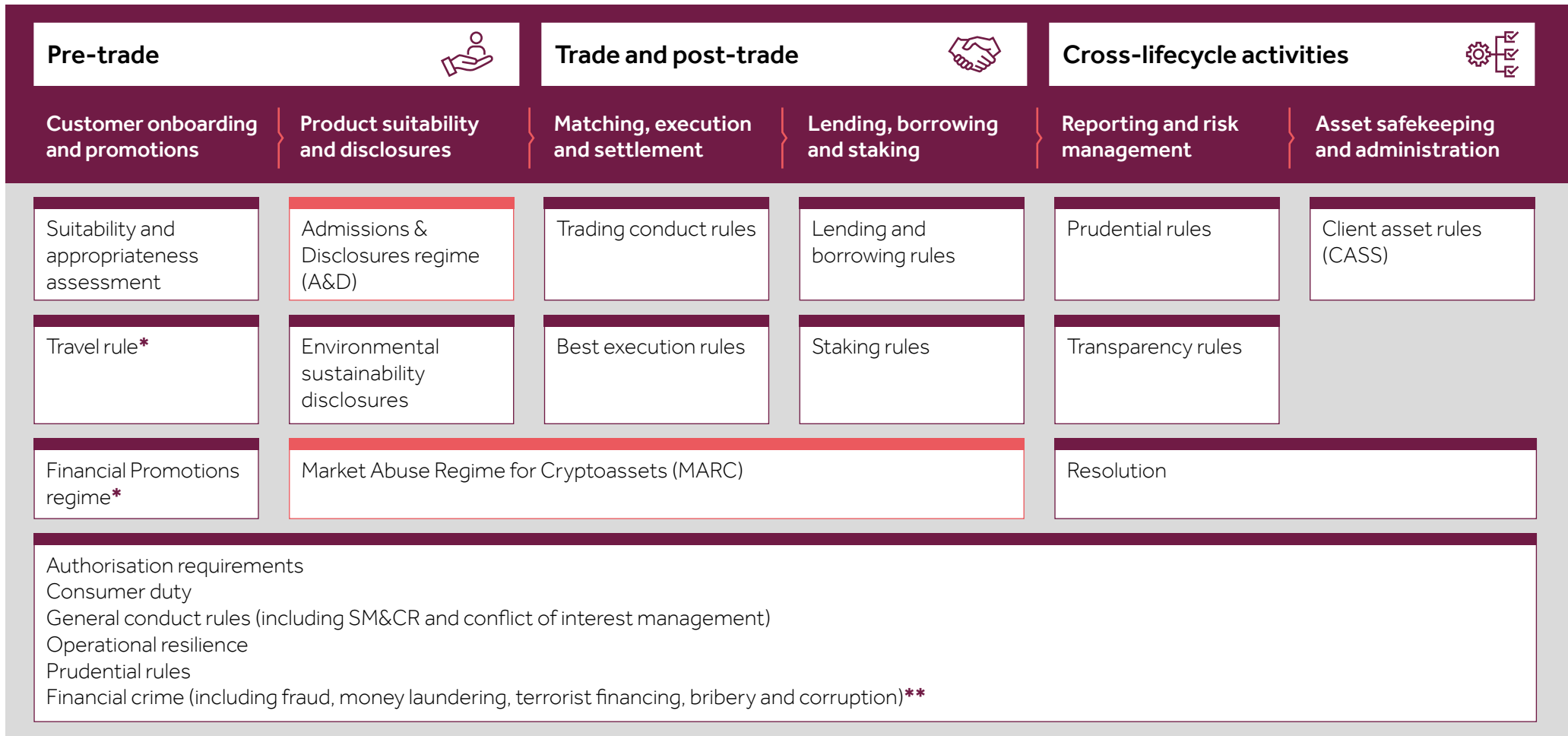
PS Policy statement



1.8 Figure 2 summarises the main parts of the current and future cryptoasset regulatory regime, highlighting those which are in focus for this DP. Separate discussion papers will be published (or have already been published, such as the [DP23/4 Regulating cryptoassets Phase 1: Stablecoins](#)) for other parts of the regime. This approach is designed to make the engagement process for external stakeholders more focused and manageable. It also reflects feedback from firms and industry associations. Our [Crypto Roadmap](#) gives further clarity on the content and sequencing of future DPs and Consultation Papers (CPs).

Figure 2. Overview of future crypto regime (not exhaustive)

- SIMPLIFIED; NOT EXHAUSTIVE -



Note: this is a high-level overview of the main 'building blocks' of the future regulatory regime, mapped against the most relevant stage(s) of the cryptoasset product lifecycle. It is not a comprehensive view of all cryptoasset activities and regulatory requirements (e.g. payment activities not represented here)

Key:

Focus of this discussion paper

Out of scope for this discussion paper

* Regime already live ** AML/CTF regime already live

- 1.9** We have engaged with industry to inform the development of our rules for the A&D and MARC regimes. We held Crypto Policy Roundtables in April and May 2024, and engaged with market participants to enable them to share their thoughts on opportunities and challenges. We considered views from these engagements in designing our proposals, which represent our initial view on the future A&D and MARC regimes. Insights from these ongoing engagements will feed into the formal consultation process. This will be initiated once the government has laid the relevant statutory instruments.
- 1.10** We haven't limited our work to domestic engagement. Internationally, we led the development of the IOSCO Crypto and Digital Assets (CDA) Recommendations, providing a baseline of global regulation for cryptoassets. We are now leading work to monitor and promote timely and effective implementation of those recommendations throughout the entire IOSCO membership. We have also undertaken significant work to develop international standards for cryptoassets through the FSB, based on the shared challenges faced by regulators globally. We will continue to collaborate with our international counterparts, sharing our insights from this consultation process and working closely through ongoing engagement with IOSCO and the FSB.

Alignment with our objectives and desired outcomes for the overall cryptoasset regime

- 1.11** We are seeking to design the regulatory frameworks for A&D and MARC in line with our objectives of consumer protection, market integrity and effective competition as set out in the 2024/2025 FCA Business Plan. We also seek to support the international competitiveness and growth of the UK economy in the medium to long term.
- 1.12** The regime will look to reduce and prevent financial crime, protect and put consumers' needs first, maintain market integrity while supporting the use of technology to help strengthen the UK's growth and competitiveness. Delivering on this ambition means taking proactive steps to manage the risks and opportunities associated with new financial technologies such as Distributed Ledger Technology (DLT) and the activities underpinning their use.
- 1.13** On the overall cryptoasset regime, we are guided by the following outcomes but acknowledge that there may be trade-offs between them.

Strategic outcomes:

- **Consumer protection:** achieve an appropriate degree of protection for the public regarding crypto products and services.
- **Market integrity:** the integrity of global financial systems is protected and enhanced.
- **Effective competition:** effective competition that delivers high quality offerings in the crypto market.
- **International competitiveness and growth:** facilitate the international competitiveness of the economy of the UK and its growth in the medium to long term, as appropriate aligning with international standards.

- **Sustainable system:** achieve sustainable stability economically, financially and environmentally.
- **Accessibility:** access to appropriate financial products and services that meet consumer needs and offer fair value.

Outcomes of regulation:

- Crypto is not attractive for money laundering, fraud, terrorism or any other criminal activity.
- Regulated firms/market infrastructure conducting cryptoassets services understand the risks (including risks to traditional finance), the regulation, the market, their customers, and design their products and/or services to achieve the above strategic outcomes.
- The firms/markets in the sector operate in a way, and demonstrate behaviours, which achieve the strategic outcomes.
- Users get communications they can understand, products and services that meet their needs and offer fair value. Users get the customer support they need, when they need it.
- The benefits and positive use cases for crypto and its underlying technology are understood by market participants. Innovation is permitted or encouraged in line with appropriate regulation to enable crypto and its underlying technology to be developed and exploited, while also looking to mitigate any risks.

Question 1: Do you agree with the outcomes we are seeking for the overall regime? Are there any important outcomes we may not have included, or any that you believe are not appropriate?

Intended benefits and potential costs of our A&D and MARC proposals

1.14 In line with our overall cryptoasset regime, our A&D and MARC proposals aim to both reduce harm and to promote market confidence, growth and sustainable cryptoasset markets by:

- improving regulatory clarity and providing stronger safeguards at the cryptoasset admission gateway
- supporting more informed decision making
- providing a well-functioning market for consumers and market participants
- reducing risks of money laundering and losses to fraud
- providing for the allocation of capital to cryptoassets on a more informed basis for consumers
- providing a well-functioning and more transparent cryptoasset market to attract more firms and help bring in more competition, drive innovation, and ultimately provide a more level playing field and enhance our international competitiveness

1.15 We anticipate our proposed approach to A&D and MARC will result in direct costs to firms, as they make changes to comply with these requirements. Incremental costs will likely involve both one-off and ongoing expenditure, and include costs associated with familiarisation, training, and firms reporting to us. Some of our proposed requirements could require changes to firms' business models, which may result in additional costs to firms. Our proposed regulation could also result in indirect costs or increased barriers to entry, which may impact competition in the sector, and result in increased prices for consumers.

1.16 We consider these potential additional costs to firms and consumers in the context of the above-mentioned potential benefits of our proposed approach. We are seeking both quantitative and qualitative input from firms so we can fully understand the costs of different approaches.

Question 2: **Do you agree with our assessment of the type of costs (both direct and indirect) which may materialise as a result of our proposed regulatory framework for A&D and MARC? Are there other types of costs we should consider?**

Question 3: **How do you anticipate our proposed approach to regulating market abuse and admissions and disclosures (see Chapters 2 and 3 for details) will impact competition in the UK cryptoasset market? What competitive implications do you foresee as a result of our regulatory proposals?**

Who should read this discussion paper?

1.17 This DP will interest anyone who has bought (or sold), or may in the future buy (or sell), cryptoassets from an entity providing services or making offers of cryptoassets in the UK or to persons in the UK. It will also interest a wide range of organisations and individuals, both domestically and internationally, that participate in the cryptoasset sector – with a focus on those interested in the wholesale aspects of the regime.

1.18 This document should be read by:

- firms or individuals, with a focus (but not exclusively) on those that participate in the wholesale cryptoassets market
- cryptoasset firms (including potentially firms based overseas) providing services to UK consumers
- traditional finance participants
- industry groups/trade bodies
- professional advisors
- law firms and accountancy firms advising on cryptoassets
- consumer groups and individual consumers
- policy makers and other regulatory bodies
- industry experts and commentators
- academics and think tanks
- other firms or professional bodies involved in cryptoassets

Equality and diversity considerations

- 1.19** Our latest Cryptoassets consumer research noted that cryptoassets owners are more likely to be male and younger – aged under 35. Those who own cryptoassets are more likely to have a higher-than-average household income.
- 1.20** Future regulation of the cryptoassets regime, would aim to reduce information asymmetries, lower the prevalence of market abuse and provide an appropriate degree of consumer protection. This could contribute to creating a wider and more diverse pool of cryptoasset consumers. Our consumer research data showed a small range of participants who bought crypto (20%) believed they had financial protection. A significant number of respondents indicated that increased regulation would make them more likely to invest in cryptocurrencies. This includes 52% of cryptoasset users and 31% of non-cryptoasset users. Both percentages comprise individuals who said they would be more inclined to invest if cryptocurrencies were more regulated, as well as those who would invest only if such regulations provided financial protection against potential losses. Increased regulation could mean that a wider, and potentially more diverse, range of people are able to benefit from using or investing in cryptoassets in a cleaner, well-functioning market. But this would come with risk, which may mean a wider range of people experience harm, including those who are more vulnerable.
- 1.21** Overall, we do not consider that the proposals would adversely affect any of the groups with protected characteristics under the Equality Act 2010 which include: age, disability, sex, marriage or civil partnership, pregnancy and maternity, race, religion and belief, sexual orientation and gender reassignment. We also believe that our proposals will not negatively impact financial inclusion.
- 1.22** We do not envisage our proposals will directly affect the digitally excluded population and older consumers as they are unlikely to invest in cryptoassets. This is supported by our cryptoassets consumer research mentioned above, noting that cryptoassets owners are more likely to be male and younger – aged under 35.
- 1.23** We expect cryptoassets consumers across all groups, not just a younger and higher-income audience, will benefit from the protection of a regulatory regime for cryptoassets from an A&D and MARC perspective. As we develop our regime, we will continue to consider if our work could affect the make-up of consumers in this market, or otherwise impact on equality and diversity. In the meantime, we welcome your input on this.

Consumer Duty considerations

- 1.24** Our Crypto Roadmap, published on 26 November 2024, noted we will consult on applying the Consumer Duty in relation to all RAO cryptoasset activities in scope of the Treasury's regime in Q3 2025. As set out in our Discussion Paper (DP23/4), we are proposing that the Consumer Duty be applied to the RAO activities of stablecoin issuance and custody for retail customers.

- 1.25** The Consumer Duty sets a higher standard of care that firms must give to their retail customers. Its outcomes-based approach allows firms to innovate and respond to technological changes and market developments while focusing on delivering good customer outcomes.
- 1.26** It applies across the distribution chain, from product and service origination through to distribution and post-sale activities. This can include firms that do not have a direct customer relationship. The Consumer Duty may apply to firms in the wholesale sector that can determine or have a material influence over retail customer outcomes. For this reason, if the Consumer Duty is applied in the same way to cryptoassets activities, this will have implications for some wholesale cryptoasset firms, for example if they have a role in the design of communications sent to retail customers. In such cases, under the Consumer Duty, we would expect firms to support retail customers' understanding by ensuring that their communications equip them to make decisions that are effective, timely and properly informed.
- 1.27** In this DP, the intended application of the Consumer Duty is particularly relevant to the A&D regime. The Consumer Duty sets a clear expectation of how firms communicate with retail customers. Beyond this, we consider it appropriate to introduce specific disclosure requirements for cryptoassets and a corresponding liability regime under the A&D regime. These will help support market participants, both retail and wholesale, in receiving consistent and adequate information about products. It will also allow us to put consumer compensation mechanisms in place to be paid by preparers of disclosure documents where they are liable for losses arising due to untrue or misleading statements.

Question 4: Do you agree with our view that while the Consumer Duty sets a clear baseline for expectations on firms, it is necessary to introduce specific A&D requirements (see Chapter 2 for details) to help support consumers?

Environmental, social & governance considerations

- 1.28** In developing this DP, we have considered the environmental, social and governance (ESG) implications of our proposals and our duty under ss. 1B(5) and 3B(c) of the Financial Services and Markets Act 2000 (FSMA 2000) to have regard to contributing towards the Secretary of State achieving compliance with the net-zero emissions target under section 1 of the Climate Change Act 2008 and environmental targets under s. 5 of the Environment Act 2021.
- 1.29** We do not consider that this DP's proposals are directly relevant to contributing to those targets. However, we recognise the impact that cryptoassets can have on energy consumption and greenhouse gas emissions. So, we have proposed disclosure requirements accordingly. We will keep this issue under review during the feedback period.

Next steps

- 1.30** We welcome feedback on the topics discussed. The questions for which we seek feedback are in Annex 1. The discussion paper period will end on 14 March 2025.
- 1.31** You can respond using the [form](#) on our website or by email dp24-4@fca.org.uk. If e-mailing, please indicate whether you wish your response to be confidential and, separately, if you are content to be named as a respondent.
- 1.32** Following this, we will consider the feedback received and conduct further industry engagement to determine our next steps. Requests for meetings can be made via the above e-mail address. We will consult in a CP on any of the proposals outlined in this DP if we propose to adopt them as part of our final rules and will draft appropriate new Handbook rules accordingly (see [FCA Crypto Roadmap](#)). Should issues arise that are beyond our powers, we will raise them with the Treasury and other stakeholders, as appropriate.

Chapter 2

Admissions and disclosures

Background and context

- 2.1** The Treasury’s consultation proposed establishing a new regime for public offers of cryptoassets and their admission to trading on a Cryptoasset Trading Platform (CATP).
- 2.2** This chapter outlines our proposals for the future cryptoasset A&D regime, including proposed requirements for disclosures by issuers or offerors at the point of admission to trading on a CATP. We discuss the proposed disclosure requirements for the dissemination of inside information under Chapter 3, which will help prevent, detect and disrupt market abuse.
- 2.3** In developing our proposals, we have considered the [IOSCO CDA Recommendations](#). In particular, we have considered recommendation 6 concerning the admission of cryptoassets to trading on a CATP.

Risks we are addressing and desired outcomes

- 2.4** The A&D regime aims to mitigate the risks and potential harms identified in the cryptoasset market. The primary risks we have identified are:
- **Financial crime (fraud, scams and money laundering):** Fraudulent or scam tokens can currently enter the UK market through CATPs, and the criminal proceeds of fraud and scams may then be laundered through cryptoassets. In 2023, according to the [Chainalysis 2024 Crypto Crime Report](#), at least US\$22.2 billion was laundered through cryptoassets, with US\$4.6 billion lost to scams and US\$1.7 billion stolen via hacks. Our proposals aim to reduce instances of fraud, scams and money laundering resulting in consumer harm.
 - **Inadequate information:** Consumers may face challenges in making informed investment decisions due to the poor quality, unreliability, inconsistency, incomprehensibility and scarcity of available information on cryptoassets. Our proposals aim to ensure consumers have the information they need to make informed investment decisions. They also make sure consumers can get compensation from the preparers of disclosure documents if the disclosures are inadequate or misleading.
 - **Market integrity issues:** The absence of transparent, high-quality, and readily available data and information may disrupt how prices are formed in markets. This results in pricing inefficiencies and potentially volatility, which raises the likelihood of losses for UK consumers. In addition, market integrity may be compromised by the misuse of cryptoassets to facilitate illicit activities, such as money laundering.
- 2.5** To mitigate these risks under the A&D regime, we propose to introduce requirements which:

- Mandate robust due diligence processes and establish procedures for rejecting admissions of cryptoassets to trading where this may result in detriment to consumers. This could reduce the risk of fraud and consumer losses.
- Support consumers in having adequate information, enabling them to make informed investment decisions.
- Set minimum standards for the market to promote fair competition between providers while ensuring appropriate levels of consumer protection.

2.6 We acknowledge that even if the A&D regime delivers the desired regulatory outcomes, some risks might remain. Disclosure alone will not fully mitigate all risks and harms within the cryptoasset sector.

2.7 For instance, while the risk will be reduced, fraud and scams may still enter the market. Consumers will need to remain vigilant when making investment decisions. Mandated disclosures should not lead consumers to complacency. They should still undertake their own due diligence and ensure the investment is aligned with their risk appetite and potential loss tolerance. Section 1C(2)(d) of FSMA 2000 reinforces this by specifying that the FCA must have regard to 'the general principle that consumers should take responsibility for their decisions'.

Question 5: **Do you agree with the risks, potential harms and target outcomes we have identified for the A&D regime? Are there any additional risks or outcomes you believe we should consider?**

Overview of the A&D regime

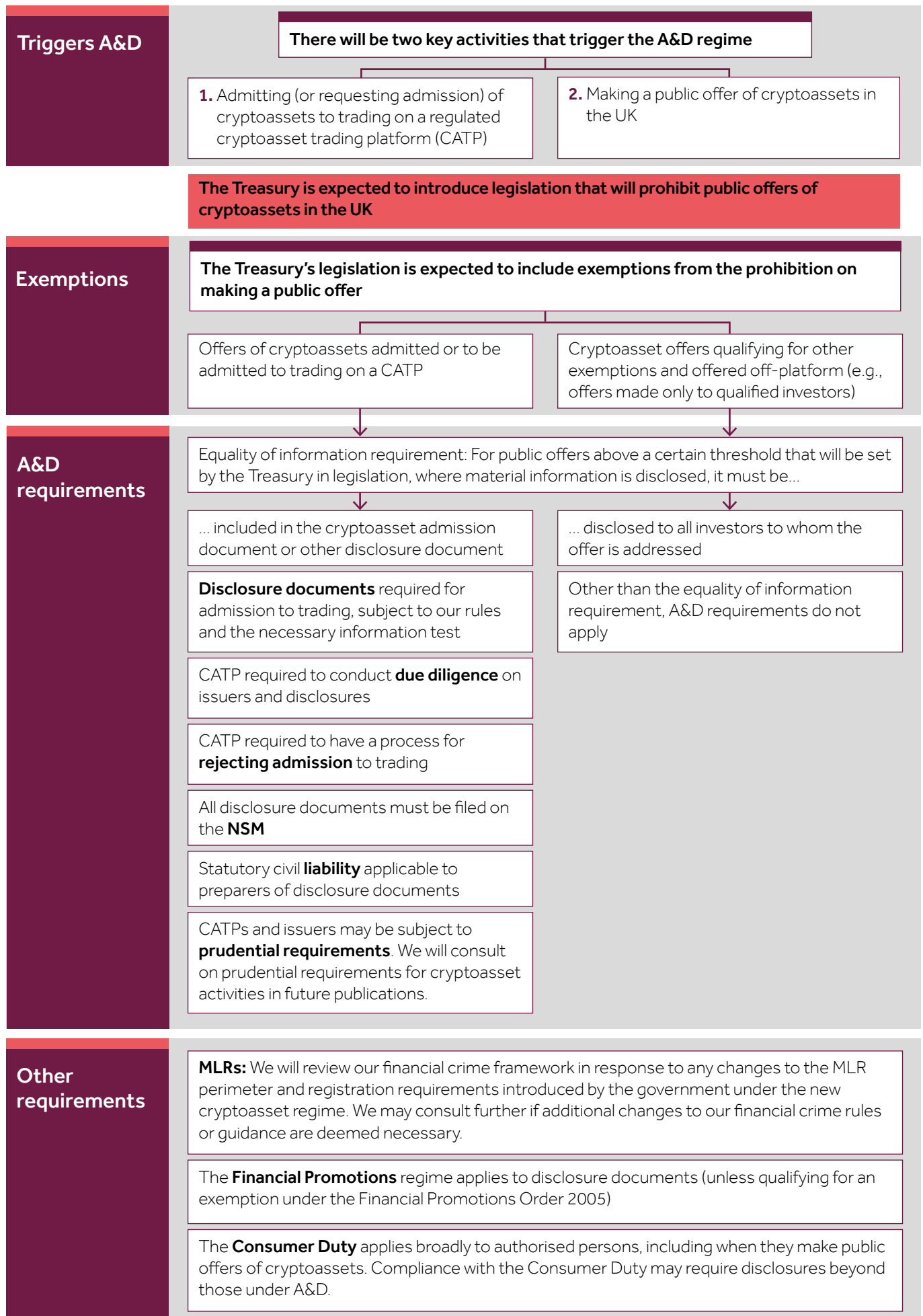
2.8 The proposed A&D regime for cryptoassets set out in this DP aligns with much of the reformed prospectus regime, which is currently under consultation in [CP24/12](#) and [CP24/13](#). However, the A&D regime will differ to account for the specific characteristics of cryptoassets.

2.9 The Treasury is expected to introduce legislation related to cryptoasset A&D covering the following:

- Making a public offer of a cryptoasset, where public offers will be prohibited unless an exemption applies. For example, when made via admission to trading on a CATP or when only available to qualified investors, such as institutional investors.
- Admitting (or requesting the admission of) a cryptoasset to trading on a CATP.
- Communicating an advertisement relating to a public offer of a cryptoasset, or the admission or proposed admission of a cryptoasset to trading on a CATP.
- Disclosing, otherwise than in an advertisement, information relating to a public offer of cryptoassets.

2.10 Figure 3 below outlines the proposed A&D regime, key exemptions, and other applicable requirements.

Figure 3. The proposed A&D regime for permitted public offers of cryptoassets



- 2.11** Existing regimes, such as the Financial Promotions regime and the Consumer Duty, are broad in scope and interact with elements of the proposed A&D regime. Similarly, the proposed future fiat-referenced stablecoins regime may also include disclosure requirements that intersect with those we are introducing under the A&D regime.
- 2.12** The A&D regime is designed to complement and align with other regulatory frameworks, avoiding duplicative requirements. To illustrate these potential interactions between the A&D regime and other frameworks, Figure 4 below outlines the key disclosure requirements across these existing and proposed frameworks.
- 2.13** We are evaluating the best approach for handling regulated stablecoins under the future stablecoin regime to avoid duplicative disclosure requirements. This is to also ensure consistency with the A&D regime and other existing regulatory frameworks. Our approach will depend on the final rules for the stablecoin regime, which we will be consulting on separately.

Figure 4. Summary of key disclosure requirements under various UK regimes

Admissions & Disclosures Regime Disclosures required for admission to trading. Content of disclosures set by the necessary information test (in legislation), FCA rules, and trading platforms' more detailed requirements.
Market Abuse Regime for Cryptoassets (MARC) (see Chapter 3) Inside information disclosure responsibilities on the issuer or person seeking admission of a cryptoasset. Requirements for issuers or persons seeking admission to disseminate inside information promptly and widely.
Fiat-referenced Stablecoins Regime (See DP23/4) Requirements for regulated stablecoin issuers to disclose: The stablecoin's full redemption policy on their website. Information on backing assets, such as value and safeguarding arrangements. Key information on the regulated stablecoin, such as stabilisation mechanisms. Information on their prudential requirements.
Conduct of Business Sourcebook (COBS under FCA Handbook) Requirements to disclose information including about the firm and its services (COBS 6) and products (COBS 13 and 14). Financial Promotions Rules: Requirements for firms to include a risk warning and risk summary on financial promotions of cryptoassets. Promotions should be clear, fair and not misleading.

Financial Promotions Guidance (See [FG23/3](#))

Cryptoasset financial promotions should include disclosure of, for example:

Key risks relevant to the cryptoasset being promoted.

Any costs, fees and charges for the products or services promoted.

Risks specific to cryptoassets that claim a form of stability (where applicable).

Where applicable, information on the backing assets, custodian and risks that the consumer will lose money if the issuer or custodian becomes insolvent.

Consumer Duty

Disclosures are necessary as part of complying with the Consumer Duty.

Requirements for firms to avoid foreseeable harm and support good consumer outcomes.

This may include disclosures beyond the disclosure requirements under other regimes such as A&D, for example, disclosures that may be necessary to support consumer understanding.

Overlap with other regimes as the Financial Promotions Regime applies to all financial promotions, and the Consumer Duty applies broadly to authorised persons

* Note that except for COBS, the Financial Promotions regime and the Consumer Duty, these disclosure requirements are subject to our future consultations.

Overview of the proposed Admissions and Disclosures Regime

- 2.14** The person who initiates the application for admission to trading would be responsible and subject to the associated liability for the production and publication of any required admission documents (including if this person is the CATP itself). The admission document would provide the core information a consumer needs to make an informed decision.
- 2.15** The CATP would undertake due diligence on the issuer, any other persons associated with the offer, and the content of the admission document. The CATP would make a summary of this due diligence public. The CATP would take its own decision, based on assessment of likelihood of consumer detriment and level of comfort from its due diligence, on whether to approve or to reject the application for admission to trading.
- 2.16** Where the CATP is the person preparing the admission document and seeking admission to trading, the admission document, due diligence and assessment of potential consumer detriment should meet the same standards as if a third-party issuer were seeking admission. In this circumstance, the potential conflict of interest should be disclosed in the admission documents.
- 2.17** Once accepted, the admission documents would be filed on the NSM.

Question 6: Should an admission document always be required at the point of initial admission? If not, what would be the scenarios where it should not be required? Please provide your rationale.

Question 7: Should an admission document be required at the point of further issuance of cryptoassets that are fungible with those already admitted to trading on the same CATP? If not, what would be the scenario where it should not be required? Please provide your rationale.

2.18 Below we discuss our specific proposals for each of these steps.

Disclosures

2.19 Consumers should have access to comprehensive, accurate and relevant information to properly evaluate whether a specific cryptoasset aligns with their investment objectives and risk tolerance. Disclosures play a key role in supporting market efficiency, improving transparency, and protecting and enhancing market integrity.

2.20 However, overwhelming consumers with excessive information may obscure the most critical details, hindering their ability to make well informed decisions. Disclosures should focus on what is truly important, allowing consumers to assess the risks and benefits effectively. Excessive disclosure can also impose disproportionate cost on the preparer, which can be passed on to the consumer.

2.21 Consumers rely on a variety of sources to gather information on a cryptoasset. Our [2024 consumer research](#) indicated that a significant proportion of consumers use online forums and social media platforms to conduct research before purchasing cryptoassets.

2.22 Information available through these sources, where communicated as part of a financial promotion, will need to comply with our financial promotion rules. This includes that the promotion must be fair, clear and not misleading.

2.23 While consumers find the information gathered from a variety of sources useful, it may be unstructured, piecemeal and not in a consistent form which allows comparison. Additionally, the financial promotions regime does not provide a liability framework. However, we can use our power under section 55L of FSMA 2000 to direct a firm to provide compensation in relation to breaches of the financial promotions regime.

Proposed rules on admission document content

2.24 As set out in the Treasury's consultation, we anticipate that there will be a 'necessary information test' set out in statute. This would be a standard applicable to the admission document, where the document preparer could be held liable for consumer losses if they did not include necessary information material to a consumer making an informed assessment of the cryptoasset. We expect that this test will require, at a minimum, disclosures on:

- features, prospects and risks of the cryptoassets
- rights and obligations attached to the cryptoassets (if any)
- an outline of the underlying technology (including protocol and consensus mechanism)
- where applicable and available, details of the person seeking admission to trading on a CATP (which may, in certain scenarios, be the CATP itself)

2.25 As with the public offers and prospectus regime in the POATRs, we are considering introducing more detailed disclosure requirements in our Handbook rules to cover information of the type set out below, as applicable or relevant. These rules could require a level of detail that is sufficient to enable a consumer to make an informed assessment of the cryptoasset across the following factors:

- The nature and scope of governance mechanisms that may affect the cryptoasset.
- The legal status of the cryptoasset, including disclosure of the classification of the asset under relevant regulatory regimes for cryptoassets or financial services.
- An identifier code for distinguishing the cryptoasset.
- The operational and cyber resilience of the cryptoasset's underlying technology and exposure to risks of hacks, vulnerabilities and disruptions. This should account for both present and future threats in severe but plausible scenarios. Such risks should be identified and documented, and any audits conducted, as well as both implemented and planned risk mitigation measures, should be disclosed.
- The key features, characteristics and methods of using the cryptoasset.
- Relevant industry standards adhered to during protocol development.
- Potential updates or changes to the protocols.
- Financial information where relevant to the price of the cryptoasset, such as the value of assets controlled by an associated treasury or foundation (where applicable), and the cryptoasset's ownership concentration and options or lock-ups for holders including insiders and affiliates (in line with IOSCO's CDA recommendations).
- The cryptoasset's track record, including trading history and major events or technology changes affecting the cryptoasset.
- The impact of the cryptoasset on sustainability related factors, such as estimated annualised energy use and estimated annualised greenhouse gas emissions.
- Where the cryptoasset makes claims to have particular sustainability credentials, the basis on which these claims are made and the evidence that supports the claims.
- Where the cryptoasset purports to maintain a form of price stability or links to a fiat currency but is not a regulated stablecoin under the future fiat-referenced stablecoins regime, a clear statement that it is not a regulated stablecoin may be required. As well as information on factors such as the total number of tokens in circulation and the backing assets. For example, backing asset composition, value, safeguarding arrangements, the most recent independent audit, how 1:1 backing is maintained (that is, assets worth an equivalent amount backing the stablecoin) and the relationship with the issuer, stabilisation mechanisms (including risks that could affect price stability), and the redemption policy with a coinholder (such as fees, type of asset or currency that is returned, timescales for redemption).

- 2.26** The above outlined requirements are designed to help firms provide sufficient detail to enable consumers to make an informed assessment. This approach offers firms flexibility in determining the appropriate disclosures based on the specifics of the cryptoasset in question. Our proposed approach also allows for adjustments over time and across different firms and cryptoassets.
- 2.27** Alternatively, we could introduce more detailed and prescriptive rules which may give more certainty that specific information is consistently disclosed across different admission documents. This would result in greater uniformity and comparability across various CATPs trading the same cryptoasset. However, this approach may lack the flexibility to adapt to the fast-changing cryptoasset market. Industry representatives at our April 2024 Crypto Policy Roundtables were generally opposed to highly prescriptive rules. They warned this could lead to impractical disclosure requirements, potentially stifling innovation and failing to account for market dynamics.
- 2.28** We propose that, subject to the necessary information test and our Handbook, CATPs would assume the responsibility of setting and implementing their own more detailed requirements for the content of admission documents. CATPs would need to review the cryptoassets' admission documents (including those they had prepared themselves) during the admission process to ensure their requirements are met. We would not be involved in assessing or approving these admission documents at the point of admission to trading on a CATP or on an ongoing basis.
- 2.29** This approach may lead to variations in admission documents across CATPs, even for the same cryptoasset. To maintain consistency, the Treasury's consultation suggested that CATPs could be required to search the NSM before new admissions and ensure information on the latest admission document is consistent with other documents previously lodged for the same cryptoasset. However, this requirement may impose additional costs and could risk perpetuating inaccuracies in existing admission documents. We agree with the Treasury's consultation that it is important to promote consistency, but we want to understand if there are other ways to achieve this.
- 2.30** For instance, an industry-led initiative to standardise disclosures would make it easier for consumers to compare cryptoassets. This suggestion aligns with feedback from our April 2024 Crypto Policy Roundtables, where industry representatives indicated that the sector could take the lead in developing standardised disclosure templates. We would be interested to understand if respondents favour this or an alternative.

Question 8: Do you agree with our proposed approach to disclosures, particularly the balance between our rules and the flexibility given to CATPs in establishing more detailed requirements?

Question 9: Are there further disclosures that should be required under our rules, or barriers to providing the disclosures we have proposed to require? Please explain your reasons.

- Question 10:** Are there any disclosures in the proposed list that you believe should not be required? If so, please explain your reasons.
- Question 11:** Do you think that CATPs should be required to ensure admission documents used for their CATPs are consistent with those already filed on the NSM for the relevant cryptoasset? If not, please explain why and suggest any alternative approaches that could help maintain admission documents' accuracy and consistency across CATPs.
- Question 12:** What do you estimate will be the costs and types of costs involved in producing admission documents under the proposed A&D regime? Are any of these costs already incurred as part of compliance with existing regulatory regimes in other jurisdictions?

Liability

- 2.31** Statements relied on by consumers must be accurate. The Treasury proposed that the persons responsible for cryptoasset admission documents (including, in some cases, the CATP itself) should be liable for their accuracy. In general, and in line with the standards in the traditional securities market, the liability standard applied will be the 'negligence' standard as under FSMA 2000 (see [section 90](#) and [schedule 10](#)).
- 2.32** This standard should give confidence to consumers that they can rely on the disclosures and a route of recourse if preparers are found, subsequently, to have provided information that was not true or accurate and the consumer suffered a loss.
- 2.33** However, the experience in traditional securities markets is that the application of this standard has created a 'chilling effect'. Preparers of admission documents may choose to avoid providing additional and decision-useful information for fear of liability. This is particularly true in respect of a reluctance to provide any forward-looking statements.
- 2.34** In line with the approach in the public offers and admissions to trading regime under the POATRs, the Treasury proposed that certain types of forward-looking statements could be treated as protected forward-looking statements (PFLS). Under the POATRs, the burden of proof rests with a consumer to establish an issuer or offeror knew (or was reckless to the fact) that a PFLS was untrue or misleading. This adopts the 'recklessness' standard of liability in FSMA 2000 [section 90A](#) and [schedule 10A](#).
- 2.35** The recklessness standard of liability imposes a lower liability risk compared to the negligence standard of liability. So, it could encourage preparers of admission documents to include helpful and relevant forward-looking information. We expect consumers to benefit from this alternative liability standard as it encourages the inclusion of more forward-looking statements in admission documents, aiding in better informed investment decisions.

2.36 We envisage the Treasury will delegate the power to us to specify which types of statements should qualify as PFLS. We outline the following types of forward-looking statements that could qualify as PFLS under our proposed rules and welcome views on the proposed approach.

- Projections, for example, the projected growth in the cryptoasset's user base.
- Intentions such as plans to upgrade the cryptoasset's underlying technology.
- Opinions on future events or circumstances, such as the anticipated impact of planned changes to other cryptoassets or technologies which may affect the cryptoasset in question.

Question 13: Do you agree with our suggestions for the types of information that should be protected forward-looking statements?

Due diligence

2.37 CATPs currently perform some due diligence before admitting a cryptoasset to trading on their platform. However, the approach is not consistent across CATPs nor necessarily in line with our expectations in the traditional securities market. This inconsistency creates risks as scams or unsuitable offers may enter the market and inaccurate information may be given to consumers.

2.38 To address these risks, we propose that CATPs should conduct a sufficient level of due diligence to assess whether a cryptoasset should be admitted to trading and that associated disclosures are accurate and complete.

2.39 This due diligence should allow the CATP to make an informed assessment of the potential risk of detriment to consumers. Due diligence should also enable the CATP to establish a reasonable level of certainty that the disclosures are true and not misleading, and whether they meet the CATP's requirements and the statutory necessary information test. The CATP would then need to use its own judgement about whether to approve the application for admission to trading.

2.40 Due diligence is also required under the Financial Promotions regime for cryptoassets intended for promotion. This ensures that promotions are fair, clear, and not misleading, and that the promoted cryptoasset is not linked to fraudulent activity, scams, money laundering or other financial crime. However, this type of due diligence remains distinct from the due diligence processes required under the A&D regime due to the differences in objectives.

2.41 In particular, due diligence under the Financial Promotions regime focuses on cryptoasset financial promotions. In contrast, the A&D regime requires due diligence on admission documents and on the issuer, offeror or person seeking admission to ensure suitability for admission. Where there is overlap between the two regimes for specific offers, the CATP will not be required to duplicate due diligence.

2.42 We are considering whether to require, in cases where the CATP itself is the person seeking admission, that the CATP should conduct due diligence. For example, to assess whether there are factors or information relating to the CATP that may influence what is appropriate to include in the disclosures or influence the decision to admit the asset. We welcome views on this and on whether CATPs should be required to assess specific factors as part of this due diligence when they are the person seeking admission.

Conducting due diligence

2.43 We propose to require firms to conduct due diligence on the offeror and the admission documents to establish a reasonable level of certainty that the offeror is legitimate, and disclosures are true and not misleading. We intend to clarify what is a 'reasonable level of certainty' in our rules and welcome input on this. We recognise that it may not always be possible to verify the legitimacy of the offeror or the accuracy of disclosures. This may be particularly so if the offeror is a third-party that might be concealing or misrepresenting information provided to the CATP.

2.44 To address the unique features of cryptoassets, we propose requiring due diligence to cover the cryptoasset's underlying technology (such as the DLT or use of smart contracts). We also want to make sure the description of risks pertinent to the cryptoasset are outlined appropriately in the admission document.

2.45 The underlying technology likely represents a key potential risk factor for many cryptoassets. We believe third-party audits of the technology could help identify these risks. As part of their due diligence, we propose that CATPs should be required to review any third-party code audits that have been conducted. This review process could involve a variety of third-party code audits, including:

- Security audits of the cryptoasset's underlying DLT.
- Tests conducted on the code (for example, through red teaming exercises) and conducted via test networks for the underlying DLT.
- Code audits on smart contract code, where applicable and relevant to the cryptoasset.

2.46 We also propose to require CATPs to conduct due diligence on the persons involved with the offer, such as the issuer, offeror or person seeking admission (where applicable and possible). This should include an assessment of their background, experience, and involvement in current or prior cryptoasset projects.

2.47 Additionally, where appropriate, firms should conduct due diligence on key individuals associated with the cryptoasset, such as members of the project team or foundation, to make sure any potential risks are identified.

Disclosure of due diligence conducted

2.48 We propose that CATPs should be required to disclose in admission documents a summary of the scope and key findings of due diligence conducted on the cryptoasset. This summary will provide consumers insights to better understand the risks associated with a cryptoasset and make informed investment decisions. The disclosures should

detail the due diligence scope and process, verify that any claims are substantiated, and cover key findings about the cryptoasset, the issuer, and other relevant persons.

2.49 CATPs should have some discretion in determining what information should be included in the summary. Some details regarding key individuals or proprietary or commercially sensitive information do not need to be disclosed. But CATPs should assess whether a summary or an extract of the findings would be appropriate to help consumers in their decision-making and maintain market integrity. This provides a balance between transparency for consumers and protection of sensitive business information.

Question 14: Do you agree with the proposed approach to our rules on due diligence and disclosure of due diligence conducted? If not, please explain what changes you would suggest and why.

Question 15: Are there further areas where due diligence or disclosure of findings should be required, or where there would be barriers to implementing our proposed requirements?

Question 16: Where third-party assessments of the cryptoasset's code have not already been conducted, should CATPs be required to conduct or commission a code audit or similar assessment as part of their due diligence process?

Rejection of admission to trading

2.50 It may be appropriate to require CATPs to have processes for rejecting admission to trading to mitigate risks within cryptoasset markets, particularly risks around fraud, scams, money laundering, and cryptoassets with potentially significant technological vulnerabilities.

2.51 Rejection decisions would need to be informed by CATPs' implementation of broader processes under the A&D regime such as due diligence. Information gathered during due diligence could support CATPs in assessing risks and the potential for consumer detriment.

2.52 We are also considering a requirement for CATPs to publicly disclose their standards for admission of cryptoassets to trading, as well as their criteria for rejecting admissions. By making these standards transparent, consumers can better understand the factors considered in the assessment process. This will help them make more informed investment decisions. These disclosures could include the areas assessed including risks and any issues that may lead to rejection of admission. These disclosures would be separate from the admission documents themselves and would not be subject to liability under the A&D regime.

Potential rules on rejection of admission to trading

- 2.53** We are considering a requirement for CATPs to reject admission of cryptoassets if they consider that there is a significant risk this may result in consumer detriment. This approach would be similar to our proposals for Public Offer Platforms (POPs) under the public offers and admissions to trading regime (see [CP24/13](#)).
- 2.54** We are considering introducing outcomes-based rules that would specify a non-exhaustive list of factors that CATPs will have to assess as part of their admission process. These CATPs will need to satisfy themselves that they understand any significant risks of consumer detriment related to these factors. Risks of consumer detriment may include, for example, material flaws in the design of the cryptoasset or its underlying technology, which might lead to a significant decrease in the value of the cryptoasset. These rules would ensure consistency and uphold high standards across CATPs when it comes to admitting cryptoassets to trading.
- 2.55** Even when a CATP complies with our requirements and conducts an appropriate level of due diligence, the CATP may still not be able to identify all potential risks that might impact the cryptoasset or detect all the issues in the admission document. However, if a CATP fails to comply with our requirements or if there is evidence of negligence or misconduct, we intend to maintain the option of taking supervisory or enforcement action where appropriate. Consumers may also have the right to take private legal action against the CATP under section 138D of FSMA 2000 for any contravention of an FCA rule.
- 2.56** Flexibility within these outcomes-based rules would allow CATPs to establish their own detailed criteria for deciding when to reject admission. This approach would allow for adaptability, accommodating differences between firms and market changes over time. We are considering rules that require CATPs to assess the following factors in their admission process:
- The background of the issuer, offeror or person seeking admission, and any key individuals responsible for changes to the cryptoasset or its network, including any potential links to fraud or scams.
 - The underlying technology of the cryptoasset, including its operational resilience and potential vulnerabilities.
 - The principal risks (technological, governance, market abuse or otherwise) which may affect the price or operation of the cryptoasset.
 - The rights and obligations attached to the cryptoasset, including the scope for these to be changed.
 - Where the cryptoasset purports to maintain price stability, the structure of its price stabilisation mechanism and the composition of any backing assets.

Question 17: Do you agree there is a need to impose requirements regarding rejection of admission to trading? If so, should the rules be more prescriptive rather than outcomes-based?

Question 18: Do you agree that we should require CATPs to publicly disclose their standards for admitting and rejecting a cryptoasset to trading? If so, what details should be disclosed?

National Storage Mechanism (NSM)

Role of the NSM

- 2.57** The NSM is our free-to-use online repository for regulated information required from issuers. It gives consumers access to information about securities and issuers under the Listing Rules, transparency rules and (parts of) the UK Market Abuse Regulation. This platform could be leveraged further by including cryptoasset admission documents in the definition of regulated information, so they would also be filed on the NSM. This would allow consumers to access relevant information when investing in cryptoassets admitted to trading on a CATP.
- 2.58** Our recent consultation [CP24/17](#) included proposals to enhance the NSM by introducing more comprehensive metadata requirements, facilitating easier access for users to find regulated information. We intend to align the A&D regime with these NSM proposals where appropriate.

Potential rules on storing admission documents on the NSM

- 2.59** We are considering requiring CATPs to make sure that all admission documents produced for cryptoassets admitted to trading on their platforms are filed on the NSM in a machine-readable format. This will enable easier analysis and extraction of relevant information.
- 2.60** We do not propose for our rules to specify the person responsible for filing the admission documents on the NSM. But we expect that the filing would typically be carried out by the issuer, the CATP or a primary information provider (PIP) (acting on behalf of the issuer or CATP). We discuss PIPs in more detail under Chapter 3.

Question 19: Do you agree with the suggested approach to our rules on filing admission documents on the NSM?

Question 20: Do you consider that the admission documents to be filed on the NSM should be in machine-readable format? If so, what format should be used to prepare the documents (for example, iXBRL or XML format)?

Chapter 3

Market abuse

Background and context

- 3.1** This chapter discusses a framework and approach for preventing, detecting, and disrupting cryptoasset market abuse. We refer to the overall regulatory approach as the Market Abuse Regime for Cryptoassets (MARC). As first set out in the government's consultation, MARC will be based on parts of the UK Market Abuse Regulation (UK MAR) tailored for cryptoasset activity. It will be designed to enhance market integrity and better protect market participants. And, it will aim to address identified risks and harms through clear and proportionate rules. Together with existing regulatory requirements on tackling illicit behaviours like money laundering, we believe MARC is integral for cleaner cryptoasset markets for UK consumers and market participants.
- 3.2** Alignment with global standards will be essential for the framework's effectiveness. This international alignment will help prevent regulatory arbitrage, where some firms might exploit differences between jurisdictions. It will also help cooperation with our international partners in tackling prevalent cross-border market abuse. A consistent regulatory baseline across jurisdictions will also benefit firms given the cross-border nature of the industry.
- 3.3** With alignment in mind, our market abuse proposals are made in consideration of the IOSCO CDA Recommendations, particularly recommendations 8 (Fraud and Market Abuse), 9 (Market Surveillance), and 10 (Management of Material Non-Public Information). Adherence with the recommendations would enable better cross-border coordination, as encouraged by Recommendation 11 (Enhanced Regulatory Co-operation).

Risks we are addressing and desired outcomes

- 3.4** The risks arising from market abuse are comparable in both traditional securities and cryptoasset markets, specifically:
- **Information asymmetries and market manipulation:** the use of abusive and directly misleading practices, such as 'rug pulls' or 'pump-and-dumps' in crypto has a direct negative impact on, and unfairly treats, consumers. The absence of repercussions exacerbates these information asymmetries and market manipulation risks. This creates an environment where consumers suffer poor outcomes, including monetary loss. In 2023, according to the Chainalysis 2024 Crypto Crime Report, 54% of new ERC-20 tokens admitted to trading on Ethereum-based decentralised exchanges displayed patterns indicative of pump-and-dump schemes.

- **Prevalence of market abuse:** the prevalence of market abuse in the cryptoasset market erodes market confidence, efficiency, and liquidity. This, in turn, limits the growth and success of the market overall, and adversely affects the outcomes for market participants.

3.5 In traditional finance, the civil market abuse regime exists under UK MAR. It prohibits the following behaviours for financial instruments: insider dealing, unlawful disclosure of inside information, and market manipulation. It also contains a definition of inside information, and additional obligations tied to inside information. This includes the requirement for issuers to disclose inside information that directly concerns them in a timely and accurate manner. It also includes the obligation for market participants to report to us suspicious transactions and orders.

3.6 As for offences under the criminal market abuse regime that covers traditional finance, criminal insider dealing is an offence under Part V of the Criminal Justice Act 1993. Criminal market manipulation is an offence under sections 89-91 of the Financial Services Act 2012.

3.7 However, as noted in the government's consultation document, there are practical limitations that prevent simply transferring the existing market abuse regime to cryptoasset markets. Key fundamental differences include:

- Highly fragmented markets increase the difficulty of surveillance (versus traditional finance, where the concept of 'main markets' and 'other markets' exists for equities, commodities, and fixed income, respectively).
- The cross-border element of cryptoassets and its highly mobile nature means that potentially abusive trading activity can occur on offshore trading platforms. This may be in a jurisdiction that does not impose equivalent cryptoasset regulations and can directly or indirectly affect price formation on UK CATPs.
- In many cases, a lack of a clearly identifiable issuer (for example, Bitcoin) to take on the same disclosure obligations that issuers do under traditional financial regulations for equities and bonds.
- Complications around identifying the 'market price' due to the decentralised nature of cryptoasset price formation or the relative lack of established methods for valuing cryptoassets.
- An absence of mechanisms to promote and support equal and transparent information for all market participants and consumers.
- Higher direct participation from retail consumers further complicating the surveillance process.

3.8 These differences complicate the creation of a market abuse regime on-par with that for traditional financial instruments. So, as also mentioned in the government's consultation, we do not consider it feasible at present to deliver the same regulatory outcomes that UK MAR does for financial instruments. What we present below for discussion instead covers what we consider a pragmatic approach to delivering a cryptoasset market abuse framework in the near-term.

3.9 Through MARC, we aim to deliver the following outcomes:

- Reduce the instances of market abuse and resulting harms to consumers.

- A common understanding of what constitutes unfair and abusive practices.
- Market participants understand their obligations to lead on taking action against abusive practices. Where market-led measures are not sufficient or available, or where regulated firms notify us of serious market abuse issues they cannot resolve, regulators may take appropriate action.
- Inside information is made available as widely and timely as possible, allowing consumers to have the same opportunities to access information and make informed decisions.
- Market participants share information such that they can identify bad actors and abusive behaviour on a cross-market basis. This will allow them to take action and prevent such abusive market behaviour from continuing. Such abusive behaviour may include instances of market manipulation, insider dealing, and other misconduct.

Question 21: Do you agree with the risks, potential harms, and target outcomes we have identified for the market abuse regime? Are there any additional risks or outcomes you believe we should consider?

Overview of MARC

3.10 The government is expected to introduce new legislation related to MARC covering the following:

- Prohibiting insider dealing in relation to cryptoassets traded on a regulated CATP.
- Requiring the disclosure of inside information relating to cryptoassets traded on a regulated CATP.
- Prohibiting market manipulation in relation to cryptoassets traded on a regulated CATP.

3.11 We also expect the government to bring the activity of operating a CATP within the scope of the Regulated Activities Order (RAO). This would enable us to require regulated CATPs to take certain actions to detect, deter, and disrupt market abuse as well as to engage with cross-platform information sharing mechanisms as discussed under the section 'Cross-platform information sharing' in this chapter.

3.12 Our policy ideas for a principles-based market abuse regime are discussed at length in this chapter, but in summary we believe this should cover:

- A regime that includes the similar offences/prohibitions as for traditional financial instruments under MAR (essentially the prohibitions on insider dealing, unlawful disclosure of inside information, and market manipulation).
- Requirements for disclosure of inside information by the issuer or other persons seeking admission of cryptoassets to trading.
- Safe harbours and exceptions for legitimate behaviours.
- Requirements on market participants for prevention, detection, and disruption of market abuse.

- Requirements for market abuse related systems and controls, particularly for CATPs and intermediaries (for example, brokers, principal trading firms, etc).
- A requirement for trading platforms to engage in information sharing to aid in deterring and disrupting cross-platform market abuse.

Prohibitions under MARC

3.13 Based on the legislative framework set out in the government's consultation, we expect that the market abuse prohibitions for cryptoassets will closely mirror those in UK MAR. With these prohibitions in place, we anticipate being granted the power to take appropriate action against these behaviours. These include prohibitions on:

- insider dealing
- unlawful disclosure of inside information
- market manipulation, including dissemination of false or misleading information.

3.14 We expect the government to base the definitions of these activities on the definitions used in the existing market abuse regime.

Question 22: **Are there any market behaviours that you would regard as 'abusive' at present, or any new abusive behaviours that may emerge, that may not be covered by the above prohibitions? Please provide examples where possible.**

Inside information disclosure responsibilities

Inside information and cryptoassets

- 3.15** Inside information, as traditionally defined under UK MAR Article 7(1)(a), refers to information which is precise, non-public, relating directly or indirectly to one or more issuers or financial instruments and which, if it were made public, would be likely to have a significant effect on the prices of those instruments.
- 3.16** The public disclosure of inside information on a continuous and timely basis is fundamental in ensuring fair and transparent markets. It fosters a level playing field for market participants. We believe this to also be important for cryptoasset markets. In the long run, we would want cryptoasset market participants to be able to trade in a fair and orderly environment with equal opportunity to act on information.
- 3.17** Necessary to this is ensuring market participants know who must disclose inside information, and when. In traditional finance, this responsibility goes to the issuer. There are however 3 key challenges in the cryptoasset space that complicate the assigning of the responsibility for public inside information disclosures. First, the absence of an identifiable issuer. Second, the likely nature of how inside information will arise in the cryptoasset space. Third, a non-issuer (typically a CATP seeking admission of a cryptoasset to trading) may admit a cryptoasset to trading without the issuer's request or consent.

Lack of an identifiable issuer

3.18 The issuer is crucial to the UK MAR obligation to publicly disclose inside information, as that issuer is most likely to create and/or be aware of information about it and its business. We believe this thinking is easily transferrable in cases of cryptoassets with easily identifiable issuers (for example, stablecoin issuers). However, this is less straightforward when dealing with cryptoassets with no easily identifiable 'issuer' (for example, Bitcoin). This makes it sometimes challenging to determine who to attribute disclosure responsibilities to. This was also a concern raised by participants at our Crypto Policy Roundtables.

The likely nature of inside information

3.19 It is important to consider how cryptoasset inside information would emerge. In traditional securities markets, inside information is not always easily identifiable. While no exhaustive list exists, market participants may benefit from reviewing our [best practice note on identifying, controlling, and disclosing inside information on traditional financial instruments](#).

3.20 Similarly, while drawing a definitive list of cryptoasset inside information would be difficult, there are certain shared characteristics. Inside information is often generated by the business activity of centralised entities, namely issuers or non-issuer CATPs that seek to admit cryptoassets to trading. For example, information on an upcoming admission of a cryptoasset to trading could constitute inside information as:

- it would be precise
- at a point in time non-public
- related to a given cryptoasset, and
- could be likely to have a significant effect on the market price of the cryptoasset.

3.21 There is also the kind of inside information defined under MAR Article 7(1)(d), that is information about a client's pending orders. For persons charged with executing cryptoasset client orders, such as intermediaries, we would require them to maintain systems and controls to protect the confidentiality of this information. We discuss this later in this chapter.

3.22 As above, a cryptoasset's admission to trading might be regarded as inside information. However, these are often admitted to trading without the involvement of an issuer. This raises the question of who should hold disclosure responsibilities in such circumstances.

The challenge of non-issuer persons seeking admission of cryptoassets to trading

3.23 In the context of this paper, non-issuer persons are any individuals or entities that seek admission of a cryptoasset but themselves do not originally create, mint, or issue the token. A lot of the time, this is a CATP but could also be a project team, community group, or a foundation. As mentioned under paragraph 2.14, the process of seeking admission of cryptoassets to trading can sometimes be initiated by non-issuer entities (a CATP,

for example). In this situation, we think the person seeking admission, who may not be directly involved in the cryptoasset's issuance, should be responsible for disclosing inside information. A challenge here, however, is that non-issuer persons do not have direct access to the same level of information as issuers themselves. Non-issuer persons may only be able to disclose inside information that they themselves are aware of.

3.24 In addition, some cryptoassets are issued through decentralised protocols or governance mechanisms, such as through a Decentralised Autonomous Organisation (DAO). These cryptoassets will lack a centralised issuer in the traditional sense to begin with.

3.25 Despite non-issuer persons not having the same level of information as issuers, there are still circumstances in which pertinent inside information might arise. For example, as suggested by IOSCO CDA Recommendation 10, and as mentioned above, information about the admission of a cryptoasset to a centralised exchange could constitute inside information which a non-issuer would be aware of.

Proposed approach

3.26 In view of the challenges discussed above, our proposed regulatory approach is that issuers who request admission to a CATP for their cryptoasset will be responsible for publicly disclosing relevant inside information. The inside information must be disclosed as soon as possible, disseminated as widely and simultaneously as possible, and through adequate channel(s) (which we discuss further in the next section below). We believe this will lead to better information symmetry and a fairer market.

3.27 Where the issuer is not identifiable, or where a cryptoasset is admitted without the issuer's request, the responsibility for disclosing inside information will fall to the person who had sought admission to trading of the cryptoasset (which we think will likely be a CATP). Our current view is that, in these cases, this responsibility should be limited to inside information which directly concerns the relevant person, and which the person is reasonably aware of. The concept of a CATP acting as this person taking up the responsibilities of an issuer in preparing an admission document, if the platform wishes to admit a cryptoasset to trading, would build on the discussion starting in paragraph 2.14 in the A&D chapter. We believe such an approach would account for the variety of cryptoassets that we expect to be admitted to trading. But we are open to market participants' views.

3.28 As a new (and relatively major) regulatory requirement, inside information disclosure responsibilities may be a challenge for issuers, CATPs, and other entities seeking admission of cryptoassets to trading. Where such persons seeking admission of cryptoassets struggle to identify inside information, this may result in information asymmetries for market participants. This challenge could be addressed with guidance, if necessary, on what falls within the definition of 'inside information' in these scenarios and needs public dissemination.

Question 23: Do you agree with our proposals to make the issuer responsible for disclosure of inside information unless there is no issuer or the issuer is not involved in seeking admission to trading?

- Question 24:** In the circumstances where there is no issuer, or the issuer is not involved with the application for the admission to trading, do you agree with our proposal that the person seeking admission to trading of the cryptoasset should be responsible for the disclosure of inside information?
- Question 25:** With regards to the second circumstance in question 24, do you agree that the person (say, 'Person A') seeking admission to trading of the cryptoasset should only be responsible for disclosure of inside information which relates to Person A and which Person A is aware of?
- Question 26:** Are the risks of information asymmetry for consumers resulting from this approach significant? Are there additional measures we need to take to further mitigate this risk?
- Question 27:** What are some examples of information that should be considered inside information? Do you think we should provide a non-exhaustive list of examples in guidance?

Additional disclosure of information responsibilities

- 3.29** Our proposals for disseminating inside information under MARC are designed to work alongside the A&D requirements for producing admission documents. Together, these frameworks aim to provide consumers with sufficient disclosure to make informed decisions. However, we recognise that certain decision-useful, non-material types of information might arise on a continuous basis, such as technological updates, that wouldn't necessarily qualify as inside information.
- 3.30** The government's consultation stated that we would consider whether ongoing disclosures should be required after a cryptoasset is admitted to trading. We remain open to this. We welcome views on whether it is necessary for regulation to specify further types of regulated information (beyond that required to be included in admission documents and inside information) that should be disclosed on an ongoing basis. This would be akin to our requirement for disclosure of financial reports etc. in our existing securities regime. Our intention would be to require decision-useful updates without duplicating the requirements for disclosing inside information. This would make sure consumers have access to relevant updates without unnecessary repetition.
- Question 28:** Are there types of information, beyond those already proposed to be made available through the A&D regime and the MARC inside information disclosure regime, that would be useful for the cryptoasset market to have access to? Please specify the nature of the information, the frequency that such information should be disclosed (if applicable), and the importance to the consumer base.

The method of disseminating inside information

- 3.31** In traditional securities markets, issuers are subject to our Disclosure and Transparency Rules which require that issuers use regulated information services to make regulated information public.
- 3.32** Important announcements and inside information about cryptoassets are often distributed arbitrarily across various social media platforms (such as X, formerly Twitter) or smaller community channels (such as Reddit). Unlike traditional finance markets, there isn't a reliable, formal channel for dissemination of inside information. This has led to the release of false or unverified information through unofficial channels, ultimately affecting price formation. Consumers may also struggle to fact-check or locate the necessary information on cryptoassets. To mitigate these risks, the government has proposed that regulated firms will be expected to release time-sensitive inside information to the public domain as soon as possible. For example, via regulated information services. This could involve consolidating all inside information updates in a single, accessible location. A centralised approach would allow for the simultaneous release of inside information to all market participants and consumers. This would help to foster a level playing field and improve market transparency, thereby mitigating potential market abuse.

Vision for channels disseminating inside information

- 3.33** A key step towards enhancing market transparency could be establishing 'formal' channels for inside information dissemination. We want to hear industry views on the most effective industry-led method for disseminating inside information to the public in a manner as wide a public as possible, and as close to simultaneously as possible. We are considering several approaches, including:
- creating bespoke crypto PIP(s)
 - using existing PIP(s) from traditional finance markets
 - publishing inside information on the firm's own website

Crypto-specific PIP(s)

- 3.34** One option is for the industry to draw on their expertise and knowledge of the underlying technology of the blockchain and take the initiative in developing bespoke PIP(s) for cryptoassets. One way to do it might be through a centralised coordinating body to coordinate the effort to set up and operate the crypto PIP(s).
- 3.35** This approach would allow for flexibility in designing PIP(s) that could meet the unique features of cryptoasset markets, while also fostering innovation and integrating RegTech solutions. For example, using blockchain technology could provide a secure, decentralised and immutable record for information disclosures, or using a unique identification code (such as a Digital Token Identifier) to identify a specific cryptoasset in disclosures made.
- 3.36** Crypto PIP(s), developed and maintained by the industry, could function on a 24/7 basis to meet the continuous trading nature of cryptoasset markets. This would enable the dissemination of inside information promptly and securely in a timely manner, allowing market participants to make informed timely decisions.

- 3.37** Traditional finance PIPs involve central regulatory oversight. But crypto PIP(s) could be industry-led, with market participants responsible for ensuring the accuracy and integrity of the information shared. Industry participants could be responsible for verifying and disseminating the information.
- 3.38** This approach could allow greater agility and innovation, empowering the market to manage information flows in a manner best suited to the unique dynamics of cryptoassets.
- 3.39** However, at our April 2024 Crypto Policy Roundtables, industry participants were concerned about the operationalisation of a crypto PIP. They noted that it takes an extensive amount of time to develop a PIP in traditional markets and might be so for developing crypto PIP(s).

Existing PIPs

- 3.40** An alternative option would be to use existing PIPs designed for traditional finance. Currently, we require PIPs to operate during set hours (7am to 6:30pm; see [Chapter 8 of Disclosure Guidance and Transparency Rules sourcebook](#)), but we understand that in theory, existing PIPs have the technological infrastructure to operate 24/7.
- 3.41** The cryptoasset industry could explore the feasibility of using existing PIPs to disseminate inside information and whether the existing infrastructure could handle the cryptoasset market's continuous 24/7 operation and trading. This option might allow the industry to leverage existing PIP(s)' infrastructure for disseminating inside information under MARC. This would significantly save resources to develop and test a bespoke crypto PIP. We welcome feedback on this approach. Particularly, from cryptoasset firms and existing PIPs, on whether using a traditional finance PIP for dissemination of inside information under MARC would be feasible and whether it could cater to the unique features of cryptoassets.

Publication on website and 'active' dissemination

- 3.42** We are assessing whether we could achieve a suitable method of disseminating inside information via market participants' publishing inside information on their websites. Publishing information simply by making it available on a firm's website may not achieve widespread dissemination with market participants. For this reason, firms would also need to actively disseminate information via the media. By 'media', we consider social media, web-based platforms and CATPs for cryptoassets to be acceptable channels to spread information.
- 3.43** 'Active' dissemination ensures widespread circulation of the information. Publication on the firm's own website can also prove the information's reliability.

Our role

- 3.44** We are open to support industry development of solutions to facilitate the timely dissemination of inside information, and we are exploring ways to help the market. We welcome expressions of interest from market participants who are interested in leading the development, testing, and where applicable, potential long-term operation of these solutions once implemented.

Question 29: Do you favour any of the options set out above? If so, which one? What are the factors that led you to this decision?

Question 30: Are there alternative options we should be considering? What might be the pros and cons of those alternative options?

Question 31: Should a centralised coordinating body coordinate the effort to help with identifying, developing and testing method(s) of disseminating inside information? If not, please provide alternative suggestions.

Question 32: Can you provide any estimated figures for costs involved with the set-up and the ongoing operational costs of any of the options?

Safe harbours and exceptions for legitimate behaviour

Background

3.45 Safe harbours under UK MAR enable certain behaviours or actions to be exempted from MAR's prohibitions. This is to prevent specific behaviours or actions, that are recognised to constitute legitimate financial activity, from being inadvertently banned by regulations. These safe harbours and exceptions can be critical for allowing markets to operate efficiently and for maintaining clear regulatory boundaries. Some existing safe harbours and exceptions under UK MAR may be adapted and carried over to MARC, where applicable to cryptoassets. For example, those concerning delaying disclosure of inside information (MAR Article 17(4)), possession of inside information and legitimate behaviours (MAR Article 9), and accepted market practices (MAR Article 13).

Principles for safe harbours

3.46 It is useful to identify the key principles that a safe harbour should meet. Such would drive the decision on whether the behaviour is legitimate and necessary to the market function. We think all cryptoasset safe harbours should meet the following principles:

- Safe harbours should only be considered if the outcome of the application of the safe harbour would support market function or financial stability.
- They should be designed to minimise the harm to consumers, including the risk of information asymmetry or consumers being misled.
- They should be specific to a well-defined activity and, ideally, be time-limited.

Question 33: Do you agree with these principles? Are there changes you would suggest? Are there others we should consider?

Addressing novel and emerging developments in cryptoasset markets

- 3.47** Technological developments and market practices in the cryptoasset space evolve more rapidly than in traditional markets. We want to keep MARC future-proof. It is important that future, legitimate market practices are not inadvertently captured under prohibitions designed to prevent market abuse.
- 3.48** At our Crypto Policy Roundtables last April and May, some industry participants highlighted the parallels between coin burning practices and share buy-back programmes. These parallels suggest that coin burning, when conducted under specific conditions, could potentially merit a safe harbour provision, similar to those granted for share buybacks.
- 3.49** For context, share buybacks are exempt under MAR Article 5. This disapplies the market abuse prohibitions related to trading in a company's own shares in buy-back programmes, subject to certain conditions in the article. We are open to considering a similar safe harbour for coin burning, provided it meets certain criteria. We welcome input on the specific characteristics of legitimate coin burning practices that would be helpful to shaping such a safe harbour.
- 3.50** Additionally, some participants at our Crypto Policy Roundtables flagged other novel features that may affect cryptoasset markets. This included Maximal Extractable Value (MEV), a topic which we have previously researched, and its nuanced types and usage. We are open to hearing views on other novel features that may affect cryptoasset markets, and that may require safe harbours or exceptions under MARC.
- 3.51** Lastly, because we expect non-issuer persons seeking admission of cryptoassets, we expect potential questions may arise on how they can use the safe harbours mentioned in paragraph 3.45. Such views may cover, for example, whether non-issuer persons have the same legitimate interests as issuers do in delaying the disclosure of inside information. We are open to hearing any such views.
- 3.52** One example of a safe harbour that could conceptually be transferred from MAR relates to backing asset shortfalls in regulated stablecoins, and delaying disclosure of this shortfall. This is particularly regarding only where a disclosure would pose financial stability risks. The considerations here mirror those in MAR Article 17(5) on the delayed disclosure of inside information about liquidity issues at a credit or financial institution, where disclosure would pose financial stability risks. Further context is also provided in Recital 52. In DP23/4 on stablecoins, we detailed requirements on the backing assets of regulated stablecoins. In particular, we highlighted the range of risks and potential impacts that could emerge if backing assets fall short of expectations. A shortfall in backing assets could affect confidence in the regulated stablecoin and cause a stablecoin 'run'.
- 3.53** If a MAR-like definition for inside information was applied, information on a regulated stablecoin backing asset shortfall could likely constitute inside information:
- the information relating to an unresolved regulated stablecoin backing asset shortfall could be precise enough to draw a conclusion on the shortfall's effect on price
 - it would be related to the regulated stablecoin and the stablecoin issuer
 - it is at a point in time non-public, and
 - it would likely have a significant effect on its peg, and therefore its price, if made public

- 3.54** Full and proper market transparency is ideal, but if the disclosure of such a shortfall in backing assets does pose financial stability risks, delayed disclosure may be justified under very exceptional circumstances. Such delay may allow the issuer to find alternative ways to manage the shortfall and avoid a 'run'.
- 3.55** We invite market participants to let us know if they believe any of the examples above or other scenarios would warrant safe harbours.

Question 34: **Should we apply the safe harbours from MAR concerning delays in disclosing inside information (MAR Article 17(4)), and possession of inside information and legitimate behaviours (MAR Article 9) to the cryptoasset market?**

Question 35: **An approach similar to the accepted market practices (AMPs) provisions in MAR Article 13 could provide flexibility to address certain crypto behaviours in the future if appropriate. AMPs, nonetheless, remain an empty set under UK MAR. Do you have any views on whether AMPs would be useful in the crypto space?**

Question 36: **What, if any, amendments to the MAR formulation of these safe harbours should we make to them to ensure they align with the principles set out above and ensure they are tailored to the cryptoasset market? Is there any additional clarity you would need us to provide over how they would apply in order to be able to rely on them?**

Question 37: **Are there other activities that we should be considering for safe harbours? Please explain your rationale including how these safe harbours would meet the principles set out.**

Market abuse systems and controls

Systems and controls in context

- 3.56** Drawing from UK MAR, our current thinking for MARC includes imposing key obligations on CATPs and intermediaries to implement systems and controls designed to address cryptoasset market abuse. This is in conjunction with obligations meant to tackle money laundering and terrorist financing under the MLRs. For interested readers, the basis for the systems and controls approach in traditional finance can be found under UK MAR Article 16 and technical standard Commission Delegated Regulation (EU) 2016/957 as contained within the Handbook.
- 3.57** We propose to take an outcomes-based approach that accounts for the size and scale of the CATPs and intermediaries' activities. This approach aligns with the government's consultation proposals. With rapid technological enhancements in cryptoasset markets,

we believe that CATPs and intermediaries will also be empowered by our outcomes-based rules to adopt innovative Regulatory Technology (RegTech) solutions for their systems and controls. This will ensure they can efficiently counter emerging new forms of market abuse threats and ideally keep the MARC framework futureproof and adaptable.

- 3.58** Our role would be to assess the effectiveness and suitability of systems and controls implemented by CATPs and intermediaries at the gateway, and ensure they continue to maintain effective and suitable systems and controls under our supervision.
- 3.59** A key distinction between our current thinking and the existing market abuse regulatory framework for financial instruments is that we do not envision a central FCA role in the receipt and assessment of Suspicious Transactions and Orders Reports (STORs). Instead, as suggested in the government's consultation, CATPs will be responsible for determining whether STORs, or an equivalent kind of reporting regime, can be deployed for their platform. This could then be used, for example, by intermediaries to report instances of suspicious transactions to the relevant CATP. CATPs would investigate suspected instances of market abuse and take relevant actions to disrupt abusive activities under their own rules.
- 3.60** We envisage the appropriate role for us, at the current scale of cryptoasset markets, is to oversee the compliance of CATPs and intermediaries with market abuse rules. This is different to the more involved role we take in traditional securities markets. Our current thinking also entails a lighter approach to regulatory notifications relative to the traditional market abuse regime. But it does not preclude the possibility of authorised CATPs and intermediaries reporting major incidents to us or for us to take direct action on particular incidents where appropriate. We would expect authorised firms to comply with [Principle 11](#) in our Handbook and disclose to us anything relating to the firm of which we would reasonably expect notice. Relevant reporting obligations, such as those under the MLRs or the obligation to file Suspicious Activity Reports, continue to also apply.
- 3.61** Our current thinking emphasises robust systems and controls at the firm level as the main mode for addressing cryptoasset market abuse. However, if firms are unable to address market abuse issues appropriately, they have an obligation to inform us, and we expect to be given the power to take enforcement action against persons where appropriate.

Question 38: Do you agree with the approach to putting the onus on CATPs and intermediaries to both monitor and disrupt market abuse? If not, why not and what alternative do you think would better achieve the outcomes we are seeking?

Market abuse systems and controls for CATPs

- 3.62** Our current thinking is to require that CATPs implement rigorous systems and controls to prevent, detect, and disrupt market abuse on their platforms. Under this approach, CATPs would be able to choose which controls, systems, and surveillance tools best suit their respective business models. We would expect CATPs to be proactive in implementing systems and controls, to conduct periodic risk assessments, and to be able to evidence these systems and controls to us as part of ongoing supervision and on request.

- 3.63** We intend to take an outcomes-based approach to this regulation and firms would be able to adjust their approach in line with the nature, size, and scale of their business. This is similar to the concept of proportionality that already exists within MAR and the MLRs.
- 3.64** We envision that one of the mediums for market abuse detection will be cross-platform information sharing, which we further discuss in the next section of this chapter. This is meant to enhance disruption of market abuse (such as through off-boarding users).
- 3.65** Some examples of systems and controls are set out in the table below, but as above we would expect the exact systems and controls a CATP implements to depend on their business model. We welcome feedback on our thinking.

Non-exhaustive list of potential CATP systems and controls

- Conflict of interest declarations.
- Personal account lists and internal rules on personal account dealing for employees (such as employees seeking clearance before trading cryptoassets).
- Information barriers.
- Employee training on overall proper management of inside information disclosures to the market concerning initial exchange offerings.
- Maintain records for 5 years.
- PDMR transaction disclosures and insider lists (for where a CATP has sought admission of a cryptoasset to trading).
- Real-time and post-trade surveillance.
- On and off-chain monitoring.
- Participation in cross-platform information sharing (see paragraphs starting from 3.80).
- Trading halts, delays, or suspensions.
- Use of emerging crypto RegTech tools where appropriate.
- Establishing platform-specific rules that set out options for disrupting abusive activity, including off-boarding clients.

Market abuse systems and controls for cryptoasset intermediaries

- 3.66** In our current thinking, intermediaries would also be required to maintain strong systems and controls to mitigate market abuse risks. We would seek for intermediaries to implement systems and controls in line with the nature, size, and scale of their business.
- 3.67** Intermediaries would be expected to proactively assess, implement, and evidence these systems and controls to us as part of ongoing supervision and on request. We envision intermediaries to produce and maintain a periodic risk assessment of their systems and controls. Intermediaries, which we would expect to become authorised entities, would be subject to the same requirements outlined in paragraph 3.60 on notifying us of any significant market abuse issues as appropriate. There will be a slight difference in the systems and controls intermediaries implement compared to CATPs. As an example, we would expect that, relative to other matters, intermediaries to be focused on ensuring the sound management of pending client orders as a primary concern.

3.68 We set out some examples of systems and controls in the table below. However, we would expect the exact systems and controls an intermediary implements to depend on their business model. We welcome feedback on this approach.

Non-exhaustive list of potential intermediary systems and controls

- Information barriers that limit access intermediary employees have to client orders to prevent frontrunning.
- Personal account lists and internal rules on personal account dealing for employees (such as employees seeking clearance before trading cryptoassets).
- Conflict of interest declarations.
- Monitoring and rejecting suspicious client orders.
- Reporting suspicious orders to the relevant CATP.
- Usage of emerging crypto RegTech tools where appropriate.
- Maintain records for 5 years.
- Contractual or other agreements with clients which would allow them to disrupt activities which they identify as abusive, including the ability to off-board the client.

Question 39: Do you agree with the areas of systems and controls where we will set outcomes-based requirements for CATPs and intermediaries? If not, which do you not agree with and why? Are there any areas where we should be considering additional systems and controls either for these firms or other market participants to achieve the outcomes we are seeking for this regime?

Question 40: Do you agree with the outcomes-based approach which allows firms to determine the best way to deliver the outcomes based on the nature, size and scale of their business?

Insider lists

3.69 We anticipate that persons seeking admission of cryptoassets, including where a CATP seeks to admit a cryptoasset on its own platform, will likely be centrally organised through, for example, a distinct legal, corporate identity. Such entities, through their roles as persons seeking admission of cryptoassets, likely will process material information in a non-public manner. This creates concepts of 'inside information' and 'insiders' relevant to that entity, and potential insider dealing risks.

3.70 The government's consultation response highlighted that obligations for managing inside information should apply to cryptoasset firms that will be regulated (such as CATPs and intermediaries). This would also apply to other market participants, such as issuers, persons acting for the issuer and persons seeking admission of cryptoassets to trading.

3.71 We think that, in all cases, firms which handle market sensitive information should have information barriers and appropriate training on the obligations for handling such information. Where there is a concentration of insider dealing risk, higher controls (in the form of insider lists) may be appropriate. Insider lists should enable management and controlled access to inside information, in addition to reliable tracking of individuals with access to inside information where needed. This should include the individual's identity, reasons for the person's inclusion on the list, the date and time of when the person gained access to inside information, and the date on which the insider list was drawn up. Insider lists could include, for example, other relevant cryptoasset information such as wallet addresses.

3.72 We believe that insider lists where used would be established by issuers and persons seeking admission as they are in traditional securities markets. They would cover both employees with access to the inside information, and advisers and any other persons acting on behalf of issuers. As an example, we would consider that CATPs should draw up insider lists where they themselves seek admission of a cryptoasset to trading.

Question 41: **Do you agree that firms involved with cryptoasset trading and market sensitive information should be subject to requirements to have appropriate training regarding the handling and control of inside information and have appropriate information barriers in place within their firms?**

Question 42: **Do you agree on the proposals regarding insider lists for issuers and persons seeking cryptoasset admissions to trading?**

Managers' transactions

3.73 Persons discharging managerial responsibilities (PDMRs) for an issuer or person seeking admission of cryptoassets to a regulated CATP would likely have access to inside information. There is a risk of PDMRs exploiting this information for unfair market gains. UK MAR in traditional securities markets requires PDMRs to disclose their transactions in relevant financial instruments. This is done through PDMR notifications, which are required to be both disclosed to us and publicly to the market. These disclosures are also useful for market participants as it provides transparency over insiders, and it also helps prevent trading in 'closed periods' (such as before the release of an issuer's year-end report).

3.74 To address the potential risk of insider dealing, there remains a question as to whether we should adapt existing UK MAR requirements to require that issuers or persons seeking admission implement systems and procedures to record PDMR transactions. And whether they should publicly disclose those transactions in a manner easily accessible to all market participants. We welcome views on whether the potential value from cryptoasset PDMR disclosures would outweigh the costs borne by issuers or persons seeking admission, or whether other alternatives could achieve similar benefits in a proportionate manner.

Question 43: Do you feel that establishing a PDMR regime for issuers/ persons seeking admission of cryptoassets would significantly advance the outcomes we are seeking at a proportionate cost?

On-chain monitoring

- 3.75** On-chain trading activity in the cryptoasset space is a key characteristic that sets it apart from traditional finance. On-chain activity can influence price formation, both directly and indirectly, across cryptoasset markets and on CATPs themselves. This makes on-chain monitoring increasingly crucial for mitigating cryptoasset market abuse. It allows real-time tracking and post-trade analysis of blockchain activities, such as transaction patterns, token flows, and wallet interactions. This level of transparency helps identify potential market abuse behaviours that off-chain systems may not singlehandedly detect.
- 3.76** While off-chain monitoring – which tracks activities such as order book trades – remains essential to provide context about users and trades, it has limitations. Illicit activities like wash trading, pump-and-dump schemes, and insider dealing often occur directly on the blockchain, avoiding detection by off-chain systems.
- 3.77** This limitation opens a gap from which market abuse can propagate. So, a wholly off-chain monitoring framework may be insufficient to fully address suspected market abuse. There is growing recognition that combining on-chain with off-chain monitoring offers a more comprehensive solution for preventing market abuse as it links up blockchain activity to real-world entities and behaviours. On-chain monitoring could, for example, provide CATP surveillance teams with better visibility over a suspicious user's trading behaviour.
- 3.78** We recognise the importance of on-chain monitoring. But, to keep the rules futureproof and adaptable to blockchain technology's evolving nature, we are cautious about making them prescriptive. We also acknowledge concerns from the industry at our Crypto Policy Roundtables on the scope of on-chain monitoring. It would be disproportionate to demand that firms scan all on-chain activity relating to a cryptoasset. Instead, our current intention is to ensure supervised firms can and do rely on on-chain monitoring where appropriate. For example, on-chain monitoring could be useful in cases where suspicious user activity involves transfers to private wallet addresses. We remain open to market participant views on this.
- 3.79** Our approach to requiring on-chain monitoring would consist of high-level rules that set out an expectation for CATPs and intermediaries to maintain on-chain monitoring capabilities. Regulated firms will be required to show these on-chain monitoring capabilities are proportionate to their business activity. But they will retain the flexibility to determine for themselves how to implement appropriate on-chain monitoring.

Question 44: Do you agree with the approach set out with regards to requiring on-chain monitoring from CATPs and intermediaries?

Question 45: Are there any aspects of systems and controls that we haven't mentioned which would help us deliver on our desired outcomes?

Cross-platform information sharing

The case for cross-platform information sharing

- 3.80** The government's consultation response has made clear the intention to facilitate through legislation cross-trading platform information sharing, taking into consideration the challenges and complexities of data sharing. We discuss below how information sharing could be used to tackle market abuse occurring across CATPs. Adopting the use of such information sharing mechanisms could provide benefits in mitigating market abuse within a fragmented market.
- 3.81** In addition, cross-platform information sharing could help align the UK with international standards. IOSCO CDA Recommendation 9 (Market Surveillance) suggests consideration of 'systems for sharing information related to suspected market abuse between relevant crypto-asset markets.' Cross-platform information sharing could also help in demonstrating controls to take prompt remedial actions on discovering market abuse, systems to detect and report suspicious behaviour, and requirements on customer due diligence – all of which are also contained under Recommendation 9. UK information sharing could also be a first step to fostering this internationally, particularly where it complements efforts to tackle illicit behaviours across borders per Recommendation 11 (Enhanced Regulatory Co-operation).
- 3.82** At present, we do not intend to establish an FCA-operated cross-platform information sharing mechanism for CATPs. We consider that the potential benefits from information sharing can be achieved through private-to-private mechanisms without our intermediation. Developing such information sharing mechanisms on an industry-led basis (instead of an FCA-led basis) will allow platforms to harness their existing expertise in monitoring cryptoasset trading activity and leverage their immediate proximity to the various products and customers. Such an approach would also allow flexibility and adoption of RegTech solutions.
- 3.83** There are examples from other areas where private-to-private information sharing has been introduced or is in use. In the UK, some information sharing between cryptoasset firms already takes place as required by the Travel Rule provisions under the MLRs. Information sharing provisions also exist in other contexts such as in the [Economic Crime and Corporate Transparency Act 2023 \(ECCTA\)](#). This enables information sharing both directly and indirectly through third-party intermediaries. Internationally, there are similar frameworks where financial institutions can share customer information with each other for the purposes of addressing suspected illicit behaviour. They include Hong Kong's proposals for information sharing among financial institutions, and Singapore's [COSMIC \(Collaborative Sharing of Money Laundering/Terrorism Financing Information & Cases\) platform](#). We therefore think there is potential for private-to-private information sharing mechanisms to mitigate potential cryptoasset market abuse.

Vision for cross-platform information sharing

- 3.84** Without mechanisms for sharing information, the value from robust market abuse systems and controls would be siloed on individual trading platforms. Cross-platform information sharing mechanisms could initially serve as information conduits to help CATPs perform better risk-based assessments of users during onboarding, and of those that are already onboarded. Combined with the existing reporting obligations that firms have under the MLRs and other legislation, cross-platform information sharing could help lead to cleaner cryptoasset markets for market participants. So, we believe some form of cross-platform information sharing should be required.
- 3.85** An effective cross-platform information sharing mechanism, coupled with rigorous market abuse systems and controls mentioned in the previous section, would significantly bolster efforts to address market abuse on and across UK CATPs. This would ultimately enhance the protection of market participants and market integrity. We envision that when a CATP identifies suspected market abuse they would be able to share relevant information about this with other CATPs. This would be done via information sharing mechanisms. This information sharing could be done, for example, after a CATP decides to offboard a user.
- 3.86** For example, if CATP 1 offboards User A, and where User A has an existing account with CATP 2, information gathered by CATP 1 on User A's suspected market abuse behaviour could be shared with CATP 2. Such information could help CATPs to make more informed decisions on whether to continue offering services to the user. If the same actor tries to onboard elsewhere, like CATP 3, the shared information from CATP 1 could be used by CATP 3 to inform onboarding checks. To prevent misuse of shared information, all CATPs in this example would be supervised by us, hence subject to our standards and expectations.
- 3.87** We consider below different potential operating models that could enable information sharing, each with their own benefits and drawbacks. They also vary in how structurally centralised they are, and in how much industry-wide coordination would be required. It may also be the case that each model's suitability varies as the cryptoasset market evolves over time, or as the number of CATPs in the UK changes.

Different operating models for cross-platform information sharing mechanisms

<p>CATPs share information about suspected market abuse through bilateral arrangements, with potential for varied formats between each agreement.</p>	<p>This is the least centralised mechanism for information sharing being considered in this table. This would provide CATPs the most flexibility in determining how information should be shared, and who to share/receive such information with. It, however, is more likely to be limited in cross-platform market abuse deterrence when compared to the 2 multilateral options below.</p>
<p>All CATPs adhere with a commonly agreed format or use open-source Application Programming Interfaces (APIs) to easily share information, but information is only shared when agreed bilaterally.</p>	<p>This operating model is similar to the first in that it requires bilateral agreements to be drawn up between CATPs. But, this could be deployed faster given agreement among CATPs to format and package shared information in the same manner.</p>

Different operating models for cross-platform information sharing mechanisms

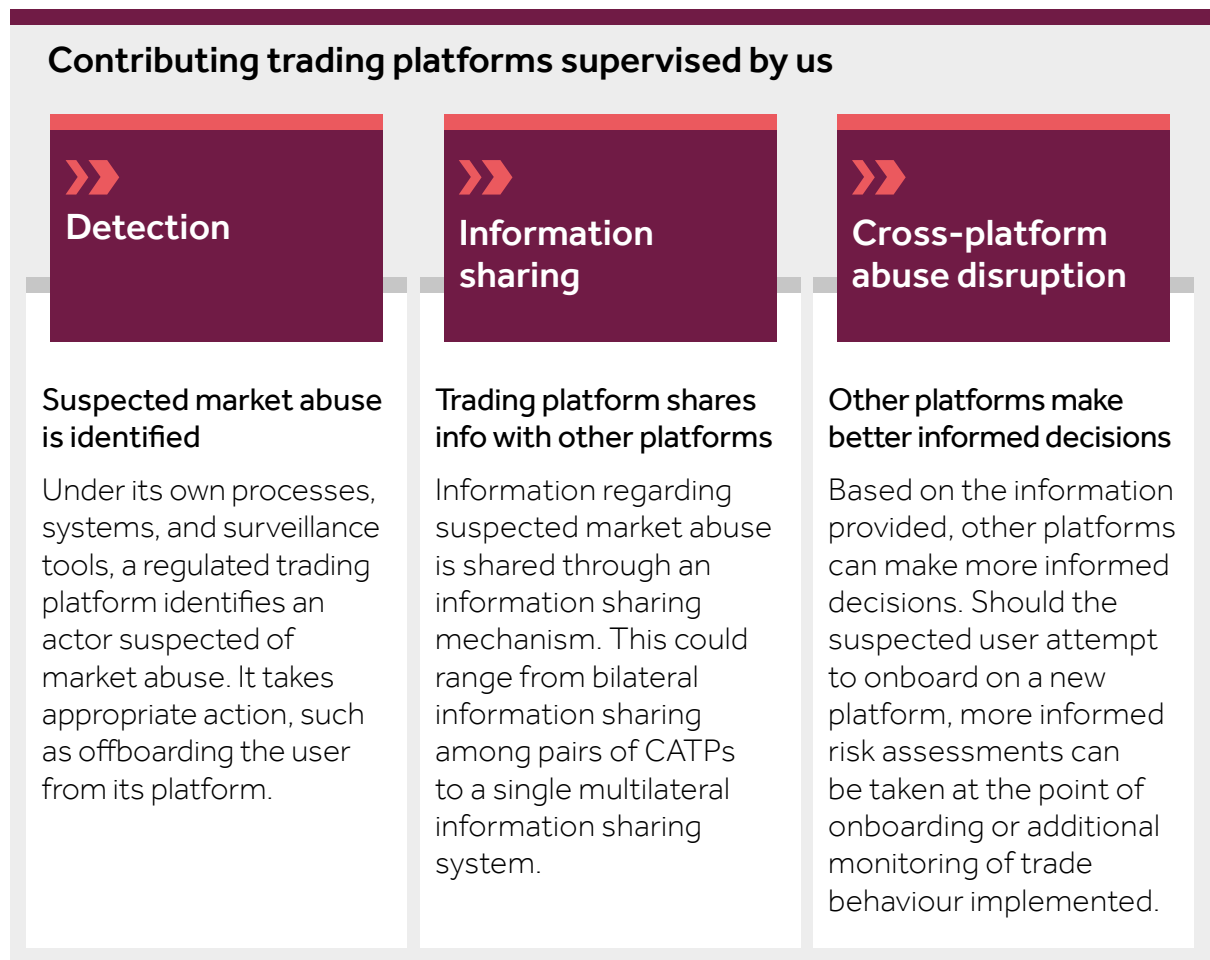
<p>Multiple multilateral cross-platform information sharing systems exist, operated by different RegTech providers or market participants.</p>	<p>This operating model entails creating systems in which more than 2 trading platforms share information with each other. In comparison to the above, this is a slightly more centralised approach to information sharing. The involvement of multiple trading platforms on a given system would also likely provide for better cross-platform market abuse deterrence. This, however, would require more industry coordination when compared to the bilateral mechanisms. This would also need the existence of multiple systems or providers.</p>
<p>One multilateral cross-platform information sharing system, or a common mechanism that enables sharing to all CATPs, is operated by industry.</p>	<p>This operating model is the most centralised of those being considered in this table. This is our preferred option as we believe this mechanism would enable the most information sharing, and the most potential deterrence of market abuse behaviour. However, as it is the most centralised of the 4 options, it would require the most industry coordination to achieve.</p>

3.88 For clarity, in any of the potential information sharing mechanisms discussed, our intent is not for information sharing to necessarily lead to automatic offboarding of a given user across CATPs. In other words, if User A is offboarded from CATP 1, and also has an account on CATP 2, we would not necessarily mandate that CATP 2 offboard User A solely on the basis of shared information. We would however expect CATP 2 to use the shared information in reaching any independent decisions it makes on its commercial relationship with User A.

3.89 The cross-platform information sharing requirements will be new to many in the cryptoasset space. During the Crypto Policy Roundtables, some industry participants expressed concerns that the identification of suspected market abuse on their platforms might be misconstrued by us as self-admission on the part of the CATP of having less rigorous systems and controls.

3.90 We do not necessarily consider identifying suspected market abuse to be an immediate indicator of such. Conversely, identifying suspected market abuse could also be an indication of a CATP's systems and controls working as intended. Any view leaning towards the former or latter will depend on the relevant context and circumstances. We encourage market participants with concerns to engage with us during the consultation process.

Figure 5. Cross-platform information sharing in action



Our role

- 3.91** At our Crypto Policy Roundtables, participants expressed the legal and technical concerns potentially posed by information sharing. These challenges include concerns around data privacy, confidentiality, and compliance with competition law, as well as ensuring compatibility with forms of data unique to cryptoassets such as wallet addresses. Cross-jurisdictional challenges and concerns about the commercial sensitivity of shared data were also brought forward, emphasising the need for a careful and rigorous framework. The industry was also concerned about the lack of a central FCA role to support the building and operating of cross-platform information sharing mechanisms.
- 3.92** We are actively considering these concerns and will continue to engage with the government on addressing them. On cross-jurisdictional concerns, we recognise that at present many jurisdictions regulate cryptoasset services through different approaches, and that expanding information sharing across borders could present challenges. Addressing some of these challenges will require the cooperation of our international partners, and could potentially be overcome with better global alignment with IOSCO CDA Recommendation 11. We continue to consider and explore what role international regulatory arrangements can play in this regard.

- 3.93** As for roundtable feedback on competition law, we remind firms of their responsibility to ensure compliance with competition law and their obligation to self-report any potential infringements as required by our Supervision (SUP) manual under SUP 15.3.32. Additionally, where there are concerns about potential infringements of competition law by other industry participants, we encourage firms to report such infringements.
- 3.94** We also recognise concerns around potentially unfairly restricting user access to CATPs due to misuse of cross-platform information sharing mechanisms. While cross-platform information sharing can help identify users involved in suspected market abuse, we also agree that it is crucial that safeguards are in place to avoid hasty decisions about offboarding users without due consideration. We would expect, under any of the 4 information sharing operating models discussed above, that CATPs subject to our supervision use the information sharing mechanisms responsibly.
- 3.95** To address operational concerns, we are open to helping support the development of industry-led RegTech solutions to design the necessary technological infrastructure for bilateral information sharing mechanisms or even a multilateral cross-platform information sharing system. We welcome expressions of interest from those who are interested in developing, testing, and potentially operating such solutions.

Question 46: Do you agree with our thinking, approach, and assessment of the potential cross-platform information sharing mechanisms discussed? Which of the options do you think is best? If none are suitable, why and what other alternatives would you suggest?

Question 47: Should a centralised coordinating body coordinate the effort to help with developing and driving forward an industry-led solution to cross-platform information sharing? If not, please provide alternative suggestions to facilitate the creation of industry-led solutions.

Question 48: We would like to gauge what further support would be useful in helping introduce cross-platform information sharing. What kind of specific regulatory input or involvement would be beneficial for the industry?

Figure 6. Sample firm journey



Chapter 4

Conclusion

- 4.1** This DP sets out our thinking on the future A&D and MARC regimes. We want to use this DP to help inform the development of a balanced regulatory framework that addresses market risks without stifling growth.
- 4.2** We would like feedback from a wide range of stakeholders, both domestically and internationally, that participate in the cryptoasset sector, with a focus on those interested in the wholesale aspects of the regime. We want to get a clear understanding of the impact our proposals could have on current business models and the market, including any relevant costs. We also want to understand if there are relevant market developments that we have not considered, or unintended consequences that could arise if we take any of the approaches suggested in this paper. We are open to hearing alternative suggestions to our proposals, if they are in line with our objectives.
- 4.3** Following the publication of this DP, we plan to engage with a wide range of stakeholders in forums as well as individual meetings. After we have considered the responses, we will draft appropriate new Handbook rules for consultation.

Question 49: Is there any further information or feedback you would like to provide to us?

Annex 1

List of questions

Chapter 1: Overview

- Question 1:** Do you agree with the outcomes we are seeking for the overall regime? Are there any important outcomes we may not have included, or any that you believe are not appropriate?
- Question 2:** Do you agree with our assessment of the type of costs (both direct and indirect) which may materialise as a result of our proposed regulatory framework for A&D and MARC? Are there other types of costs we should consider?
- Question 3:** How do you anticipate our proposed approach to regulating market abuse and admissions and disclosures (see Chapters 2 and 3 for details) will impact competition in the UK cryptoasset market? What competitive implications do you foresee as a result of our regulatory proposals?
- Question 4:** Do you agree with our view that while the Consumer Duty sets a clear baseline for expectations on firms, it is necessary to introduce specific A&D requirements (see Chapter 2 for details) to help support consumers?

Chapter 2: Admissions and disclosures

- Question 5:** Do you agree with the risks, potential harms and target outcomes we have identified for the A&D regime? Are there any additional risks or outcomes you believe we should consider?
- Question 6:** Should an admission document always be required at the point of initial admission? If not, what would be the scenarios where it should not be required? Please provide your rationale.
- Question 7:** Should an admission document be required at the point of further issuance of cryptoassets that are fungible with those already admitted to trading on the same CATP? If not, what would be the scenario where it should not be required? Please provide your rationale.

- Question 8:** Do you agree with our proposed approach to disclosures, particularly the balance between our rules and the flexibility given to CATPs in establishing more detailed requirements?
- Question 9:** Are there further disclosures that should be required under our rules, or barriers to providing the disclosures we have proposed to require? Please explain your reasons.
- Question 10:** Are there any disclosures in the proposed list that you believe should not be required? If so, please explain your reasons.
- Question 11:** Do you think that CATPs should be required to ensure admission documents used for their CATPs are consistent with those already filed on the NSM for the relevant cryptoasset? If not, please explain why and suggest any alternative approaches that could help maintain admission documents' accuracy and consistency across CATPs.
- Question 12:** What do you estimate will be the costs and types of costs involved in producing admission documents under the proposed A&D regime? Are any of these costs already incurred as part of compliance with existing regulatory regimes in other jurisdictions?
- Question 13:** Do you agree with our suggestions for the types of information that should be protected forward-looking statements?
- Question 14:** Do you agree with the proposed approach to our rules on due diligence and disclosure of due diligence conducted? If not, please explain what changes you would suggest and why.
- Question 15:** Are there further areas where due diligence or disclosure of findings should be required, or where there would be barriers to implementing our proposed requirements?
- Question 16:** Where third-party assessments of the cryptoasset's code have not already been conducted, should CATPs be required to conduct or commission a code audit or similar assessment as part of their due diligence process?
- Question 17:** Do you agree there is a need to impose requirements regarding rejection of admission to trading? If so, should the rules be more prescriptive rather than outcomes-based?
- Question 18:** Do you agree that we should require CATPs to publicly disclose their standards for admitting and rejecting a cryptoasset to trading? If so, what details should be disclosed?

- Question 19:** Do you agree with the suggested approach to our rules on filing admission documents on the NSM?
- Question 20:** Do you consider that the admission documents to be filed on the NSM should be in machine-readable format? If so, what format should be used to prepare the documents (for example, iXBRL or XML format)?

Chapter 3: Market abuse

- Question 21:** Do you agree with the risks, potential harms, and target outcomes we have identified for the market abuse regime? Are there any additional risks or outcomes you believe we should consider?
- Question 22:** Are there any market behaviours that you would regard as 'abusive' at present, or any new abusive behaviours that may emerge, that may not be covered by the above prohibitions? Please provide examples where possible.
- Question 23:** Do you agree with our proposals to make the issuer responsible for disclosure of inside information unless there is no issuer or the issuer is not involved in seeking admission to trading?
- Question 24:** In the circumstances where there is no issuer, or the issuer is not involved with the application for the admission to trading, do you agree with our proposal that the person seeking admission to trading of the cryptoasset should be responsible for the disclosure of inside information?
- Question 25:** With regards to the second circumstance in question 24, do you agree that the person (say, 'Person A') seeking admission to trading of the cryptoasset should only be responsible for disclosure of inside information which relates to Person A and which Person A is aware of?
- Question 26:** Are the risks of information asymmetry for consumers resulting from this approach significant? Are there additional measures we need to take to further mitigate this risk?
- Question 27:** What are some examples of information that should be considered inside information? Do you think we should provide a non-exhaustive list of examples in guidance?

- Question 28:** Are there types of information, beyond those already proposed to be made available through the A&D regime and the MARC inside information disclosure regime, that would be useful for the cryptoasset market to have access to? Please specify the nature of the information, the frequency that such information should be disclosed (if applicable), and the importance to the consumer base.
- Question 29:** Do you favour any of the options set out above? If so, which one? What are the factors that led you to this decision?
- Question 30:** Are there alternative options we should be considering? What might be the pros and cons of those alternative options?
- Question 31:** Should a centralised coordinating body coordinate the effort to help with identifying, developing and testing method(s) of disseminating inside information? If not, please provide alternative suggestions.
- Question 32:** Can you provide any estimated figures for costs involved with the set-up and the ongoing operational costs of any of the options?
- Question 33:** Do you agree with these principles? Are there changes you would suggest? Are there others we should consider?
- Question 34:** Should we apply the safe harbours from MAR concerning delays in disclosing inside information (MAR Article 17(4)), and possession of inside information and legitimate behaviours (MAR Article 9) to the cryptoasset market?
- Question 35:** An approach similar to the accepted market practices (AMPs) provisions in MAR Article 13 could provide flexibility to address certain crypto behaviours in the future if appropriate. AMPs, nonetheless, remain an empty set under UK MAR. Do you have any views on whether AMPs would be useful in the crypto space?
- Question 36:** What, if any, amendments to the MAR formulation of these safe harbours should we make to them to ensure they align with the principles set out above and ensure they are tailored to the cryptoasset market? Is there any additional clarity you would need us to provide over how they would apply in order to be able to rely on them?
- Question 37:** Are there other activities that we should be considering for safe harbours? Please explain your rationale including how these safe harbours would meet the principles set out.

- Question 38:** Do you agree with the approach to putting the onus on CATPs and intermediaries to both monitor and disrupt market abuse? If not, why not and what alternative do you think would better achieve the outcomes we are seeking?
- Question 39:** Do you agree with the areas of systems and controls where we will set outcomes-based requirements for CATPs and intermediaries? If not, which do you not agree with and why? Are there any areas where we should be considering additional systems and controls either for these firms or other market participants in order to achieve the outcomes we are seeking for this regime?
- Question 40:** Do you agree with the outcomes-based approach which allows firms to determine the best way to deliver the outcomes based on the nature, size and scale of their business?
- Question 41:** Do you agree that firms involved with cryptoasset trading and market sensitive information should be subject to requirements to have appropriate training regarding the handling and control of inside information and have appropriate information barriers in place within their firms?
- Question 42:** Do you agree on the proposals regarding insider lists for issuers and persons seeking cryptoasset admissions to trading?
- Question 43:** Do you feel that establishing a PDMR regime for issuers/ persons seeking admission of cryptoassets would significantly advance the outcomes we are seeking at a proportionate cost?
- Question 44:** Do you agree with the approach set out with regards to requiring on-chain monitoring from CATPs and intermediaries?
- Question 45:** Are there any aspects of systems and controls that we haven't mentioned which would help us deliver on our desired outcomes?
- Question 46:** Do you agree with our thinking, approach, and assessment of the potential cross-platform information sharing mechanisms discussed? Which of the options do you think is best? If none are suitable, why and what other alternatives would you suggest?

- Question 47:** Should a centralised coordinating body coordinate the effort to help with developing and driving forward an industry-led solution to cross-platform information sharing? If not, please provide alternative suggestions to facilitate the creation of industry-led solutions.
- Question 48:** We would like to gauge what further support would be useful in helping introduce cross-platform information sharing. What kind of specific regulatory input or involvement would be beneficial for the industry?
- Question 49:** Is there any further information or feedback you would like to provide to us?

Annex 2

Glossary

Term	Definition
Authorised Person	A person who has Part 4A permission to carry on one or more regulated activities.
Blockchain	A type of distributed ledger which records transaction information in 'blocks', distributed amongst a network of nodes that work together to reach consensus on updates to the shared ledger, creating an auditable 'chain' of transactions.
Coin Burning	Taking cryptoassets out of permanent circulation by means such as sending cryptoassets to a wallet with no access key etc.
Designated Activities Regime (DAR)	The DAR framework enables the government to 'designate' activities, and to give us rule-making, supervisory and enforcement powers over these activities.
Inside Information	Defined in the Market Abuse Regulation under MAR Article 7.
Issuer	Under the Market Abuse Regulation, an issuer means a legal entity governed by private or public law, which issues or proposes to issue financial instruments, the issuer being, in case of depository receipts representing financial instruments, the issuer of the financial instrument represented.
Insider Dealing	Defined in the Market Abuse Regulation under MAR Article 8 and prohibited under MAR Article 14.
Market Manipulation	Defined in the Market Abuse Regulation under MAR Article 12 and prohibited under MAR Article 15.
Minting	Creating new digital coins or tokens on a blockchain network.
Peg	A stablecoin's targeted reference value (e.g. 1:1 with the US dollar).
Regulated Information	All information which an issuer, or any other person who has applied for the admission of financial instruments to trading on a regulated market without the issuer's consent, is required to disclose under: a. DTR; or b. Articles 17 to 19 of the Market Abuse Regulation; or c. Listing Rules.

Term	Definition
Unlawful Disclosure of Inside Information	Defined in the Market Abuse Regulation under MAR Article 10 and prohibited under MAR Article 14.
Wallet	A device or service that stores users public and private keys, allowing them to interact with various blockchains and to send and receive cryptoassets.

Annex 3

Abbreviations used in this paper

Abbreviation	Description
A&D	Admissions & Disclosures
CATP	Cryptoasset Trading Platform
CP	Consultation Paper
DAR	Designated Activities Regime
DLT	Distributed Ledger Technology
DP	Discussion Paper
DTRs	Disclosure Guidance and Transparency Rules
ECCTA	Economic Crime and Corporate Transparency Act 2023
EU	European Union
FCA	Financial Conduct Authority
FSMA	Financial Services and Markets Act
IOSCO	International Organization of Securities Commissions
MARC	Market Abuse Regime for Cryptoassets
MLRs	The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017
NSM	National Storage Mechanism
PDMR	Persons Discharging Managerial Responsibilities
PIP	Primary Information Provider
RAO	Regulated Activities Order 2001
RegTech	Regulatory Technology
UK MAR or MAR	Onshored Regulation (EU) No 596/2014, or the Market Abuse Regulation

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 020 7066 6087



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

