FCA Discussion Paper Response

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

14th March, 2025

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

Via e-mail: dp24-4@fca.org.uk

Re: Discussion Paper Response
Regulating cryptoassets: Admissions & Disclosures and Market Abuse Regime for Cryptoassets

Dear Wholesale Cryptoasset Policy Team,

Shift Markets welcomes the opportunity to contribute to this discussion paper and play a role in helping shape the UK's evolving regulatory landscape. We commend the FCA for its forward-thinking approach with its cryptoasset roadmap, ensuring that its requirements and oversight remain adaptive and responsive to the dynamic financial landscape.

The consideration of A&D and MARC frameworks in relation to cryptoassets represents a significant advancement toward regulatory clarity and standardisation. This step not only enhances the UK's regulatory landscape but also positions the country as a leader in fostering a secure and reliable environment for cryptoassets.

Robust regulatory frameworks are strengthened through active industry engagement and sustained public-private collaboration. Our aim is to contribute meaningfully to the development of a regulatory framework that benefits all stakeholders and supports the continued growth and innovation of the cryptoasset sector. We fully support the FCA's objectives of promoting market integrity, protecting consumers, and fostering effective competition. These priorities align closely with our commitment to advancing industry standards and fostering a crypto ecosystem that is secure, transparent, and sustainable. Leveraging our extensive expertise as an infrastructure provider in the cryptoasset space, coupled with our deep understanding of the industry's challenges and opportunities, we are dedicated to providing valuable insights and practical recommendations.

This submission reflects our proactive commitment to advancing a more agile and forward-looking approach to digital assets, contributing to the enhancement of the financial ecosystem. We are eager to support the FCA in developing guidelines that not

only elevate industry standards but also uphold the principles of transparency, resilience, and adaptability in the rapidly evolving cryptoasset space.

Our response takes into consideration themes of market protection, interoperability, standardisation and clarity for market participants. Overall, we advocate for a regulatory approach that recognises the unique features of cryptoassets yet embraces a level of technology neutrality when considering economic functions and associated risks. By aligning these principles with the FCA's objectives, we aim to contribute meaningfully to the development of a robust and balanced regulatory framework that supports innovation while safeguarding the integrity of the financial system.

About Shift Markets

Shift Markets provides trading technology, market access, and regulatory solutions for businesses operating in traditional and digital asset markets. We equip clients with trading environments allowing customisation of liquidity, compliance tools and user management, enabling them to scale securely and meet evolving regulatory requirements. Shift Markets is dedicated to helping clients achieve their goals and establish strong, lasting operations in the crypto industry. Our expertise encompasses crypto exchanges and forex brokerages, enabling businesses to navigate the complexities of digital finance with security and efficiency.

Shift's services are designed to support every stage of launching and operating a trading platform, including market making, regulatory guidance, and ongoing technical support. By integrating financial expertise with regulatory strategy, we support the long-term stability and growth of digital asset businesses. Our mission is to make blockchain-based finance accessible and scalable for businesses of all sizes—whether market leaders or new entrants—through proven technology, strategic guidance, and industry expertise.

Shift Markets remains at the FCA's disposal for further dialogue and we look forward to continued engagement with the FCA in shaping the future of cryptoasset regulation in the UK. Please do not hesitate to contact us at legal@shiftmarkets.com should you require any further clarification or expansion on any of the points mentioned.

Sincerely,

Olohirere Longe
Senior Counsel, Regulatory
Shift Markets

Overview

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?

We support the strategic outcomes outlined by the FCA and believe they provide a strong foundation for the development of a robust regulatory framework. However, we suggest that strengthening infrastructure and fostering growth and innovation should be explicitly included as additional strategic outcomes. Furthermore, the industry requires greater transparency in regulatory rules and a clear path forward, which we believe should also be a defined regulatory objective.

We agree with the proposed outcome where *'crypto is not attractive for money laundering, fraud, terrorism or any other activity'* as strong anti-money laundering protections and controls are key contributors towards healthy financial ecosystems. However, we believe this should be rephrased. To support this goal, we recommend rephrasing the language to focus on the development of clean and effective AML controls. The current phrasing risks perpetuating the misconception that crypto is inherently linked to criminality, whereas, in reality, blockchain technology enhances transaction transparency. Rephrasing the objective to emphasise strengthening AML frameworks shows a more active regulatory approach and also reiterates to market participants that they bear a responsibility in maintaining and abiding by those frameworks. For instance, one of the aims suggested is to improve regulatory clarity and provide stronger safeguards - this would be a good outcome for the regulation in terms of phrasing. This approach, aimed at improving regulatory clarity and providing stronger safeguards, would more effectively communicate the intent of fostering a clear and compliant environment.

More clarity or direction could be provided to the outcome that *'firms /markets in the sector operate in a way, demonstrate behaviours, which achieve the strategic outcomes'*. We recommend adopting more specific and evidential language. For instance, requiring firms to implement demonstrable policies, procedures, and controls for anti-money laundering and countering the financing of terrorism (AML/CFT) and in alignment with MARC could provide clearer benchmarks. Additionally, encouraging the use of tools to identify and manage associated risks would help firms better assess their progress and align with regulatory expectations. Having more measurable outcomes may make monitoring their effectiveness easier and better establish a minimum baseline for conduct.

Enhancing these areas will align more closely with the FCA's strategic outcomes, supporting the prevention of financial crime, promoting consumer protection, and maintaining market integrity while fostering growth and healthy competition in the UK.

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?

Overall, yes. However, more could be considered.

Compliance costs certainly apply. Compliance costs are a significant factor, particularly for firms operating across multiple jurisdictions. These firms may face the need for greater harmonisation and standardisation of processes to align with the regulatory framework. Some firms may find it easier to adopt the strictest standard across the organisation for uniformity, which may result in firmwide adjustments if the UK's standards are the most stringent. Firms may likely need to invest in new or upgraded reporting tools to meet enhanced requirements.

Further, firms may incur additional legal or advisory costs as they adapt their service offerings to align with the new regulatory framework. This could include seeking advice on compliance, regulatory expectations, operational changes, and cross-jurisdictional alignment.

Hiring and training are also important considerations. There may be a need to hire more staff to manage compliance, reporting, and monitoring obligations effectively. Linked to compliance, another cost worth considering is training. Training is essential, particularly for firms transitioning from traditional fiat service offerings to crypto-specific markets. Specialised training providers may be required to deliver programmes that address the unique features of crypto market abuse and surveillance. Formal training on specific surveillance techniques and systems should also be considered. With training, the quality of market abuse detections as well as an understanding of A&D should improve, which will enhance investor confidence and staff efficiency.

Customer education and information dissemination may incur additional costs for market participants. Entities may need to update marketing materials, websites, and literature to reflect the new regulatory requirements. This will ensure that clients and stakeholders are informed of the changes and their implications.

Some smaller firms may face increased barriers to entry with more upfront financial investment associated with technology, staffing and training. However, with clear principles of proportionality and ensuring that systems and controls are fitting for the nature and scale of operations, this should be manageable. Costs may also vary depending on the client type as institutional and retail customers present distinct risks and requirements. Entities will need to tailor their systems to address these differences effectively, which may result in varying costs.

Investment in technology infrastructure will be necessary to support the listing of cryptoassets and implement trade surveillance software that accounts for the nuances

of crypto markets. Interconnected tools that integrate with broader financial services offerings will also be critical. Given the 24/7 nature of the crypto market, firms will need robust screening tools and systems capable of continuous transaction monitoring. This will likely require additional investment. Regardless, any costs should be proportional to the size, scale and nature of operations.

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?

The outcomes could drive and promote competition with more players in the market as well as provide necessary clarity on the regulatory expectations.

Admissions & Disclosures

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?

We agree with the classification of financial crime, inadequate information and market integrity risks as primary risks.

To address risks associated with inadequate information, disclosures, risk warnings, and token vetting policies and procedures should be subject to regulatory review. The outcomes could be further strengthened by incorporating minimum threshold standards for issuance of assets. These standards should particularly consider customer types, with stricter limits applied to retail customers to ensure greater protection, compared to institutional or professional investors. Additionally, the outcomes should include minimum disclosure requirements, as these measures would significantly mitigate the risks posed by inadequate information.

Regulatory reporting and monitoring of transactions and activities are also essential outcomes. These would play a key role in addressing financial crime and market integrity risks. Minimum thresholds and disclosure requirements would specifically help mitigate the risks associated with inadequate information. We agree that the due diligence measures already proposed in this Paper are well-suited to addressing the financial crime risks identified.

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.

Yes it should be required at the point of initial admission for the purposes of standardisation. This should be for assets admitted or to be admitted to trading on a CATP. This will help potential investors make more informed decisions.

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.

No, not always. Requiring an admission document at the point of further issuance of a fungible asset may be overly burdensome. If the asset is fully fungible, meaning it is indistinguishable from previously issued assets in terms of risk, mechanism, characteristics, function, and value, and the only difference is the time of issuance, a new admission document may not be necessary. In such cases, the risks associated with the asset would have already been identified and disclosed, so a new admission document may be redundant. The key word is fungibility. If there are differences in aspects such as mechanism, value, or other characteristics that could impact the risk profile of the cryptoasset, these differences should be disclosed as these differences could affect fungibility and possibly the investment outcome. In such instances, transparency is critical.

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?

We agree that flexibility is essential to accommodate innovation in the cryptoasset market and promote fair competition in the markets. Admissions are resource intensive and accommodations should be made for smaller firms which will often lack the resources which are at the disposal of institutional players. The minimum disclosures work towards creating a baseline framework. It should be made clear that those four points are necessary information material to a consumer making an informed assessment of the cryptoasset. Focusing on the features, rights, outline of underlying technology and details of the person seeking admission to trading should be sufficient.

While the additional details in section 2.25 serve as a useful guide, a clear distinction must be made between these guidelines and the obligations under Consumer Duty. The additional flexibility benefits firms in structuring their disclosures, but it should be

made clear that this is not a regulatory shortfall that could be interpreted as a breach of Consumer Duty. The informed assessment needs to be more precise when looking at consumer duty because a balance should be struck between consumer protection preventing the opening the floodgates of litigation. This is particularly important to avoid undue exposure for smaller firms or undue pressure on institutional players.

10. Are there any disclosures in the proposed list that you believe should not be required? If so, please explain your reasons.

Potential updates or changes to protocols could be excluded, as they are inherently difficult to predict or track at this stage. Instead, it would be more practical to address such changes through ad hoc notifications as and when they arise. This approach ensures that firms are not burdened with speculative disclosures while maintaining the ability to inform stakeholders promptly and effectively when updates occur.

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.

There should be consistency but searching the NSM may not achieve that goal as information could still be missed and it may be challenging to oversee or verify as different entities may have different standards for their search. Having minimum standards and a template may be more beneficial.

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?

The costs associated with producing admission documents under the proposed A&D regime encompass several key areas, including compliance, legal advice, cyber resilience audits, resource allocation, and the use of third-party software.

Compliance costs are significant, as firms may need to engage third-party auditors to verify financial and operational disclosures, ensuring adherence to the regime's requirements. While some of these costs may overlap with existing regulatory obligations in other jurisdictions, the specific demands of the A&D regime could necessitate additional audits or expanded scopes especially with cryptoassets if they were not accounted for previously. Legal advice is another critical component, as firms

will require counsel to draft and review admission documents, ensuring they meet disclosure obligations. Firms with an international presence may already incur legal costs for similar purposes, but the unique aspects of the A&D regime could lead to increased expenses.

Further, a deeper cyber resilience audit may be required to evaluate the security and robustness of the platform listing the cryptoasset, ensuring compliance with cybersecurity and data protection standards. Time and resources will be needed to compile and verify historical data on the cryptoasset, including track records and trading history, which may involve internal teams or external consultants. Specialised third-party software may be necessary to gather and analyse this data. While firms with existing compliance frameworks and tools may find some overlap, the A&D regime's specific requirements could still result in additional costs. Having scalable tools or consolidating compliance processes may be a way to manage these costs.

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

Overall, yes. Projections are a key consideration when making an investment decision but also subject to change due to a number of external factors, and so should be protected. With rapidly changing technology, this is a necessary protection. Instead, firms should maintain up-to-date information on their websites and ensure broad communication to users when technological changes occur

Forward-looking statements should be protected to prevent excessive litigation. We agree with this approach, as it strikes a balance between an entity’s ability to provide useful general information and consumers’ ability to assess that information in their investment or trading decisions, without exposing firms to undue liability.

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.

We agree with the proposed approach to due diligence rules, particularly the emphasis on third-party audits, which offer a reasonable degree of independence and enhance transparency. Public access to these audits will aid in risk assessment by clearly outlining findings and deficiencies, enabling informed decision-making.

However, due diligence on individuals involved presents challenges. Background checks generally require the subject's consent, and their scope (i.e. negative news or watchlist checks) should be carefully considered to ensure relevance. While open-source information is accessible, it may not always be pertinent or beneficial. It could be more practical to focus on the entity itself unless key individuals have chosen

to be listed on specific platforms. Conducting checks on the issuer, offeror, or person seeking admission is more manageable and relevant.

Although the proposal suggests conducting due diligence on the project team or foundation *'where appropriate'*, this could exceed many firms' risk appetites. Extending this to project team members or foundation participants is unnecessarily burdensome, as these individuals may no longer be involved or may not have continuous influence over the project, leading to confusion rather than clarity. An audit of the protocol and related systems should suffice in most cases.

Regarding the disclosure of due diligence, a written audit report could be required, with the focus on identified risks rather than the firm's specific due diligence processes. A summary or extract of key audit findings should suffice, rather than a detailed account of the due diligence process itself. Individual opinions on persons involved vary by firm and risk appetite, and such details may be unnecessary. Requiring extensive disclosure could also complicate and unnecessarily prolong the listing process. However, potential or actual conflicts of interest and how they are addressed need to be disclosed in detail to help investors make informed decisions. Similarly, risk disclosures such as information on crypto trading decisions, technical, cyber and operational risks, should be clear and available.

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?

Admission forms should be included with a set template. Following Financial Stability Board guidance, there should be disclosure of clear transparent information regarding governance framework, operations, risk profiles and financial conditions.

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?

This may be overly burdensome depending on the circumstances. Making the assessments available as soon as practicable may afford firms more flexibility. It need not be required but firms can opt to do so and have a statement of that position so it is clear to consumers. This helps towards fair competition as additional barriers with excessive audits can be limiting.

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?

There should be a risk based and informed approach guiding admission or rejection bearing in mind the consumer duty. Rejection is up to the issuer or entity in a similar position based on the set risk appetite.

Assessing '*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*' is too broad. At a minimum, it could be limited to the issuer, offeror, or person seeking admission. Additionally, the definition of '*background*' could be more specific and focus on relevant factors such as experience in issuing similar assets, track record, or AML/CFT risks, rather than an overly broad inquiry into personal history which may be irrelevant. If the assessment of an individual's background is considered in determining whether to admit or reject an asset, the focus should remain on the project or asset rather than personal histories, to prevent investment decisions from being driven by personalities. Deep investigations into individuals may be considered in limited cases where they hold a controlling stake or their role is explicitly relevant to the asset or network. The rest of the admission process rules should remain unchanged.

Nevertheless, we believe that investigations into individuals are largely unnecessary and that the focus should remain on the entity and the asset itself to ensure a fair and efficient admission process.

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?

We disagree. Firms may have proprietary standards and this disclosure may negatively affect competition. Alternatively, minimum or summarised information could be provided as guidance for investors to better understand what the CATPs standards are. In other instances, such standards could be made available upon request which balances the interests firms may have with proprietary standards, and the need for transparency and informed decisions for investors.

Market Abuse

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?

While we agree that information asymmetries and market manipulation are risks arising from market abuse, *'prevalence of market abuse'* comes across as more vague. The real risks here appear to be erosion of market confidence, efficiency, and liquidity - so it may be worth rephrasing to provide more specificity whilst remaining broad enough to accommodate future changes.

Lack of transparency also poses a risk, as it may be unclear what is driving prices or what inside information would be relevant for a consumer or investor. In such instances, investors and consumers are left in a state of uncertainty. This opacity can lead to uninformed decision-making and create unfair market conditions. Another critical risk is the possible facilitation of money laundering, as market abuse can create opportunities for illicit financial activities and in turn threaten the integrity of the financial system.

Risks to market stability/market volatility may also be worth including. This is especially relevant since market abuse can destabilise markets, resulting in inefficiency and overall volatility. Asset prices could become susceptible to rapid changes and fluctuations, while distorted supply and demand dynamics contribute to instability.

In terms of outcomes, transparency is worth explicitly noting. It ensures that market participants have access to accurate and relevant information, fostering fair market participation and competition. Additionally, transparency facilitates information sharing among market participants, enabling them to identify bad actors and abusive behavior across markets. This strengthens market oversight and enhances the overall integrity of the financial system. The outcome of having *'market participants share information such that they can identify bad actors and abusive behaviour on a cross-market basis'* is linked to transparency but such transparency should be clearly included in the phrasing. Transparency contributes towards fair market participation and fair competition for players.

Established controls and procedures to prevent market abuse and the establishment of clear reporting of instances of market abuse with remediation is an outcome worth considering. Such mechanisms support accountability and work towards creating a level playing field for all market participants, supporting fair competition and reducing the risk of manipulation.

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.

We believe the information is sufficient. However, updates should be made annually so market participants know there is a set time to expect an update - this positively contributes towards standardisation and setting expectations for consumers.

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?

We support *'using existing PIPs from traditional financial markets'* for uniformity. This avoids unnecessary compliance and reporting burdens on issuers and market participants - especially those that operate across multiple asset classes, such as crypto CFDs and traditional financial instruments. A unified system that accommodates cryptoassets in turn simplifies reporting obligations and eliminates the inefficiencies associated with managing multiple platforms. This approach also reduces the compliance and reporting burden on issuers, making it a more practical and efficient option.

A mixed existing PIP allows for better comparisons across firms, enabling users to assess disclosure history for a range of asset types and entities. It also mitigates selective disclosure, reduces information asymmetries, and promotes consistency in how information is issued. Greater accessibility and oversight from an external body work to enhance the credibility and timeliness of disclosed information. Standardised formats improve comprehension for retail users while making the process more efficient for institutional investors. Adjusting existing PIPs to accommodate crypto-specific features is a more practical and streamlined approach than creating a separate crypto PIP. Since existing PIPs already have the technological infrastructure to operate 24/7, they can be adapted to meet the needs of the crypto market and adding crypto-specific elements to these platforms is more efficient and cost-effective than building a new system from scratch. This integration allows crypto participants to align with established financial infrastructure more quickly, fostering innovation and market stability. The unique characteristics of cryptoassets can be addressed through collaboration with industry stakeholders. Engaging with industry stakeholders works to ensure that the tools and frameworks developed for reporting inside information are tailored to the needs of the crypto market, without needing to create a separate bespoke crypto PIP.

'Publishing inside information on the firm's own website' is also a workable option. This is especially so given the larger retail base in cryptoasset markets. Websites are a natural and expected source of information about a company, making them an accessible tool for retail consumers who may not be familiar with centralised PIPs. Retail investors are more likely to seek information directly from a company's website, which aligns with the need for accessibility in a market with a large retail presence. Further, websites serve as a direct and immediate channel for firms to communicate updates, ensuring timely dissemination of information. This is a positive as it reduces delays in accessing critical disclosures. Publishing information on the website also affords firms more control and flexibility. Firms can tailor the presentation and timing of their disclosures to align with their broader communication strategies. This autonomy allows companies to maintain consistency in their messaging and adapt to the specific needs of their client base.

However, the website route may face challenges of fragmentation. While websites may be effective for individual firms, they require investors to visit multiple sources to gather information, which is less efficient than a centralised repository. This fragmentation can hinder the ability of market participants to access and compare information across firms. Again, with websites, reliability and bias are rightly noted additional concerns. Firms may adopt a more conservative or selective approach to disclosures compared to the standardised formats used in centralised PIPs. This lack of standardisation can create inconsistencies in the timing and format of updates, making it difficult for investors to determine when new information is available. Such inconsistencies hinder comparability and analysis, particularly for institutional investors who rely on uniform data for decision-making. Media distribution is another consideration when it comes to the autonomy of website disclosures. The media distribution aspect may be a straightforward option for institutional players but could be particularly challenging for smaller firms with limited resources. Nevertheless, publishing inside information on a firm's website remains a viable option, particularly for retail accessibility, autonomy, and direct communication. The success of this method would work better in some contexts compared to others.

PIPs are relevant to ensure there is a standard format and dissemination mechanism for market participants. *'Creating bespoke crypto PIP(s)'* would mean that the information is specialised just for the crypto aspect; however, it is more practical and efficient to utilise the already established PIPs. First, this may allow more flexibility for current traditional financial market participants to engage with cryptoassets as issuers could deal with both traditional and cryptoassets. A single PIP that accommodates both types of assets simplifies the process for issuers and market participants. It eliminates the need to navigate multiple platforms, reducing complexity and ensuring a more streamlined approach. While a bespoke crypto PIP might offer agility and innovation, it would also lead to greater fragmentation within the market. This fragmentation could result in inefficiencies, such as the need to search across multiple registers (traditional

PIPs, bespoke crypto PIPs, and firm websites). It could also contribute to information overload, making it harder for market participants to access and analyse relevant data. Furthermore, separating crypto disclosures from traditional financial disclosures may undermine the legitimacy of crypto markets, as it creates a perception of divergence rather than integration with established financial systems. It is also rightly noted that the launch time for a bespoke crypto PIP could be delayed as industry participation and specific buildouts will be needed - here it may be more proactive and efficient to update an existing system.

The primary objectives of transparency and stability in financial markets can be achieved through the use of traditional PIPs. Adapting existing PIPs to include crypto-specific elements ensures consistency, reduces confusion, and maintains unified standards across the market. A unified approach using existing PIPs and possibly also firm websites, promotes market efficiency, cohesion, and accessibility.

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.

Yes, a centralised body could coordinate with input from industry players to inform direction and act as an information resource.

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?

It is important to maintain the option for authorised CATPs and intermediaries to report significant incidents to the FCA. This is especially important as those trading traditional securities may also be trading cryptoassets and this disclosure is important for the transparency and general overview of particularly threatening participant activity. Reporting major incidents of market abuse minimises large information gaps. The FCA could provide guidance on what it considers a major incident, and could issue functional templates to assist CATPs and intermediaries when preparing STORs related to major incidents.

It makes sense for CATPs and intermediaries to both monitor and disrupt market abuse on every transaction and order which they are directly involved in. CATPs and intermediaries should evaluate their level of influence or dominance within a particular cryptoasset market segment, especially considering the European Securities and Markets Authority's draft technical standards relating to market abuse. Based on this evaluation, they need to ensure that their arrangements, systems, and procedures for

preventing and detecting market abuse are appropriate for their level of influence in the market.

The prevention, monitoring, detection, and identification of suspicious orders and transactions may be delegated to a group entity or service provider. However, the systems implemented by these entities must be thoroughly assessed to ensure they are adequate and comply with regulatory requirements. The authorised firm is still responsible for ensuring these systems are adequate and compliant with regulations. To effectively prevent market abuse, it is essential to establish appropriate trading rules that contribute to its mitigation.

Additionally, firms must implement a clear and structured assessment procedure to determine what constitutes reasonable grounds for suspicion or escalation. This ensures consistency and accountability in identifying and addressing potential issues. Here, robust compliance systems are critical. Firms must adopt systems that include real-time surveillance of trading activities, enabling the timely detection and reporting of potential market abuse.

To ensure market integrity and protection, it is crucial to have a level of central oversight for major incidents, and a clear regulatory escalation process. Market abuse is a significant risk that necessitates supervision, checks, and balances. A minimum standard for reporting to the regulator should be established. The current reporting requirement is not overly burdensome.

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?

Overall, yes. Conflict of interest declarations are a critical component of maintaining market integrity. Firms must ensure that such declarations are comprehensive and transparent, identifying and addressing any potential conflicts that could compromise decision-making or regulatory compliance. There should be robust systems and controls to eliminate or manage material conflicts of interest such as related party transactions.

Information distribution may be useful to add to the systems and controls. This is especially helpful to monitor unlawful disclosure of inside information and to control particular market abuse risks. Market participants must disclose any information that could affect prices as soon as possible, except in cases where immediate disclosure would prejudice the legitimate interests of the issuer, the offeror, or the person seeking admission to trading. This requirement imposes significant obligations on monitoring the provision of information to the market.

Given the existence of pump-and-dump schemes with cryptoassets, often coordinated online via social media or private groups, it is essential to establish clear information channels and monitoring mechanisms to detect and prevent market abuse. Social media and the ability to trade any day any time are crypto specific risks - the markets are always open, and so oversight is necessary. Information distribution affects marketing as well and firms should ensure marketing communications are not misleading, as issuing false or misleading statements constitutes fraud and a form of market abuse. When it comes to information distribution and trade transparency, firms could display real-time bid and offer prices along with the depth of trading interest. Additionally, post-trade data such as transaction prices, trade times, and volumes could be made available.

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?

Yes. We believe proportionality is a key guiding outcome and principle.

41. Do you agree that firms involved with cryptoasset training 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?

Yes. To prevent insider trading, entities must implement strict controls and monitoring mechanisms to detect and prevent trading based on inside information that could influence the price of cryptoassets. Comprehensive policies and procedures should be established to prevent the unauthorised dissemination of information. Regular training for employees is essential to reinforce these measures, enabling better monitoring and identification of risks. Such training equips staff to identify, prevent, and report market abuse effectively, while also enhancing their ability to meet regulatory reporting requirements and share relevant information with third parties. This ensures that employees are well-prepared to cooperate with regulatory authorities during market abuse investigations, including granting access to records, communications, and other key data.

Market manipulation negatively impacts market integrity and includes actions such as manipulating benchmarks, or engaging in deceptive trade practices. To better manage and prevent such manipulation, firms must implement robust compliance systems including training on how to identify these situations. These also include thorough recordkeeping of all transactions and trading decisions for review and investigation, as well as the use of advanced surveillance tools. Policies and controls should establish information barriers and ethical walls to ensure that information is shared only in

authorised manners. Training, stress testing and internal reviews help test the efficacy of these systems.

Comprehensive training programs are critical for staff involved in the prevention, monitoring, detection, and identification of suspicious orders, transactions, and other activities that could indicate market abuse. Training should be conducted regularly and be proportional to the size and scale of the business. It is also essential to strike a balance between human intervention and technological review. While automated systems are valuable for detecting potential threats, human analysis is indispensable for identifying patterns that technology may overlook. This dual approach ensures a more effective response to threats, even if it incurs additional costs, as it reduces the risk of false alerts and enhances the overall integrity of the system.

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

Yes. To protect market integrity and safeguard from manipulative practices, insider lists are important. Insider lists play a vital role in developing and maintaining a robust supervisory system to safeguard material non-public information. This includes preventing front running and trading ahead by establishing effective information barriers and controls to prevent information leakage and the misuse of sensitive information.

Management of non-public information involves several key measures. Firms must implement controls to restrict access to material non-public or sensitive information on a need-to-know basis, such as through the use of ethical walls. Periodic reviews should be conducted to assess who has access to non-public or market-sensitive information, ensuring that access is limited to authorised individuals. Additionally, firms should establish processes to facilitate whistleblowing and the reporting of breaches to regulators, which enhances risk management and improves the monitoring of information flows.

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

Yes. We agree that on-chain monitoring is key for detecting market abuse. The rules governing on-chain monitoring should be established by market participants to ensure they are practical and adaptable. Overly prescriptive rules can hinder flexibility and stifle technological innovation, so it is essential to allow room for advancements in monitoring systems. On-chain monitoring should be employed where appropriate, supported by tools designed to detect and address market manipulation, market sounding, and insider trading.

Effective monitoring systems should include features that automatically identify suspicious trades, generate alerts for compliance teams, and provide detailed analyses to verify whether flagged trades constitute unlawful behavior. Firms must avoid lapses in their monitoring responsibilities, such as failing to adequately track customer activity for patterns of manipulation, neglecting to review surveillance exception reports, or overlooking non-surveillance sources of red flags, such as regulatory inquiries, service provider feedback, or publicly available information about known manipulators. Additionally, firms must ensure that responsible staff are properly trained to identify and address potential issues.

General guidelines for monitoring, whether on-chain or off-chain, should require firms to tailor their procedures to supervise differing sources of order flow effectively. This includes proprietary trades, retail customers, institutional customers, and foreign financial institutions. Procedures must be sufficiently detailed to document the escalation of issues, evaluate the effectiveness of alerts, and track STOR trends. On-chain monitoring should also incorporate real-time surveillance of market activity to ensure timely detection and response to potential abuses.

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

Firms should avoid several critical deficiencies that could compromise their ability to detect and address manipulative conduct effectively. There should be established procedures that are reasonably designed to identify patterns of manipulative conduct. These procedures should clearly define specific steps for monitoring such behavior and assign responsibility to designated individuals or teams. Additionally, there should be clear escalation processes to address detected manipulative conduct, ensuring appropriate actions are taken promptly and consistently.

Surveillance controls are also worth noting and firms should design and implement robust surveillance controls capable of capturing manipulative trading activities. These controls should be tailored to the firm's operations and market conditions. Regular evaluations of these controls are essential to ensure their adequacy, particularly in light of changes in the customer base, market dynamics, or emerging trading practices.

It is also necessary to maintain and review customer and proprietary data to detect manipulative trading schemes. This includes identifying activities such as front running, trading ahead, spoofing, and prearranged trading. To ensure the controls remain effective, there should be periodic assessment of the adequacy of controls and thresholds.

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?

In relation to the proposed operating models, our views are as follows:

'CATPs share information about suspected market abuse through bilateral arrangements, with potential for varied formats between each agreement': This approach is highly fragmented and does not effectively promote industry-wide information sharing. While it does provide significant flexibility, it falls short of achieving the desired outcome of comprehensive information exchange due to its limited scope and reach. For this system to be more effective, it is essential to incorporate a broader range of information sources. Expanding the scope of information sharing would enhance its success by fostering greater collaboration and ensuring that all relevant data is accessible across the industry.

'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': APIs facilitate interoperability with other technological infrastructures, enabling seamless integration and communication between systems. By allowing information to be shared only when explicitly agreed upon, APIs provide robust control and protection, ensuring that sensitive data does not fall into the wrong hands or get disseminated unnecessarily. This controlled approach enhances data security and aligns with regulatory requirements. APIs may also be more favourable as often multiple of regtech providers may be involved and this creates a level of standardisation which is needed in order for information sharing to be effective. However the bilateral aspect is a restriction and information may not flow as freely or there may be delays with information sharing which could hinder timely decision-making and market responsiveness. To maximise the effectiveness of this option, third-party providers must demonstrate sufficient expertise and a deep understanding of the trading markets in the relevant region. Overall this method could positively contribute towards interoperability and secure information sharing.

'Multiple multilateral cross-platform information sharing systems exist, operated by different RegTech providers or market participants': This option offers greater flexibility in selecting RegTech providers, which in turn fosters positive competition and encourages new entrants into the RegTech market. Such competition is beneficial for innovation and efficiency within the space. Given the importance of cohesion and partnerships in the RegTech ecosystem, this alternative is both practical and workable. Technology infrastructure providers often maintain established relationships with

relevant RegTech providers, and leveraging these relationships can streamline processes for firms. For instance, if two CATPs use the same RegTech provider, said provider should be able to facilitate smooth information sharing between the two platforms. This interoperability enhances operational efficiency and supports market integrity. Having multiple multilateral cross-platform information sharing systems can promote healthy competition and ensure that firms have access to diverse solutions tailored to their needs. On an operational level, it can also significantly improve onboarding processes and information sharing for client verification prior to establishing relationships. This is a clear benefit for market participants, as it enhances transparency and reduces delays.

'One multilateral cross-platform information sharing system, or a common mechanism that enables sharing to all CATPs, is operated by industry': The primary advantage of this approach is that it fosters collaboration, consensus, and uniformity among participants. These elements are essential for creating a cohesive and standardised framework that benefits the broader market. The downside is the process of collaboration and achieving consensus can be time-consuming. The burden on early participants may be significant, as would be responsible for laying the groundwork and driving the process forward. Additionally, this method may delay implementation/go-live since it requires extensive coordination and agreement among all parties involved.

In contrast, multiple multilateral information-sharing systems offer a more immediate solution. These systems are essentially "plug and play". The onus could be on the RegTech providers to share information amongst themselves. Also, cross platform information sharing shouldn't necessarily mean offboarding flagged instances as different firms have varied risk appetites. Again proportionality should be top of mind as the risk appetite depends on nature and scale of business.

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?

Interoperability of systems is key for cross platform information sharing. The type of information collected and how this is collected varies according to jurisdiction. There should be constant input from industry players to make sure the most pertinent information is collected and standardised while affording firms much needed operational flexibility.

Conclusion

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

Regular industry engagement is important to foster fitting regulation, innovation and standard setting. Clear roadmaps as the FCA has done, are beneficial for firms to ready themselves for changing regulations and discussion and consultation papers with industry thought leadership contribute towards a more critical and nuanced approach to regulation and regulatory compliance.

When considering risks, despite the technicalities of cryptoassets, it is important for firms, depending on the client base, to disclose, in a clear and concise non-technical manner, all material sources of operational and technological risks. This is particularly critical for those targeting retail markets, where accessibility and transparency are paramount. The FCA should also mandate the implementation of appropriate risk management frameworks, encompassing people, processes, systems, and controls, to effectively manage and mitigate these risks in this regard.

In line with technicalities, and in general service provision, to better address cyber and system resilience, firms should adopt robust measures that are reviewed regularly. These measures could include the establishment of an operational and technology risk management framework and the implementation of frequent and rigorous code audits to mitigate cybersecurity risks. Such practices ensure that firms remain resilient against evolving threats and maintain the trust of market participants.

Overall, safeguards should align with those applicable to traditional financial services where there is no functional or technological difference, adhering to the principle of "same activity, same risk, same regulation/regulatory outcome." This alignment ensures consistency, fairness, and regulatory coherence across financial markets.