Joint Response to the FCA's Discussion Paper DP25/1 - Regulating Cryptoasset Activities

June 13, 2025

Executive Summary

This response is a joint effort by the IOTA Foundation, the International Association for Trusted Blockchain Applications (INATBA) and the Cardano Foundation to provide an industry perspective on the FCA's proposed cryptoasset regulatory framework. As organisations actively operating in the cryptoasset industry, this submission reflects our shared industry perspectives and insights. We deeply appreciate the opportunity to comment on these important proposals.

We support the FCA's goal of enhancing consumer protection and fostering a safe and regulated cryptoasset market in the UK. However, we are concerned that the definitions and exact scope of the regulatory regime lack clarity, and that the prohibitions it would introduce would stifle innovation and reduce the competitiveness of the UK cryptoasset market overall, especially in the area of decentralised finance (DeFi).

In particular, we respectfully recommend that the FCA provide a clear differentiation between custodial service providers on the one hand and non-custodial services on the other hand. Based on our direct involvement in building and operating these technologies, we firmly believe that non-custodial models and decentralised infrastructures warrant a different regulatory approach compared to custodial and centralised services. Applying identical regulatory measures across fundamentally different models threatens to push innovation offshore and would prove incompatible with the foundational architecture of decentralised technologies.

Firstly, with regard to staking, the current proposal does not differentiate between custodial staking services and protocol-native staking mechanisms that do not involve any third-party custody or control. The vague wording of "making arrangements for qualifying cryptoasset staking" proposed in the Treasury's draft *Financial Services and Markets Act 2000 (Regulated Activities and Miscellaneous Provisions) (Cryptoassets) Order 2025* lacks nuance and risks extending the regulatory scope to an undefined group of network participants. We respectfully recommend that the FCA take this opportunity to clarify that non-custodial, native staking should fall outside of the regulatory regime, and that only custodial staking

services, where the service provider controls the cryptoassets on behalf of the user, should be regulated.

Secondly, with regard to cryptoasset lending and borrowing, we propose that the proposal should clearly differentiate between the risks posed by centralised lending and borrowing services and those posed by decentralised environments. In this context, we respectfully disagree with the proposed intention to restrict firms from offering access to cryptoasset lending and borrowing products to retail users, as these services play an important part of the evolving open financial ecosystem.

Thirdly, with regard to DeFi, we believe that international competitiveness and growth go hand in hand with innovation. All DeFi protocols and related applications begin as centralised projects in one way or another. In order to develop, they must be allowed to grow and evolve towards true decentralisation. From our collective experience within the industry, we believe that DeFi services would be better regulated through self-regulation. In February 2025, INATBA published a proposal for DeFi self-regulation (DeFi Self-Regulation: A Proposal for the Industry), setting out effective ways to tackle the risks that the FCA seeks to regulate. We believe that voluntary self-regulation is more impactful in achieving the market safety standard that policy makers across Europe aim for, without hampering the growth and competitiveness of the market.

In our response, we highlight our concerns around the proposed banning of retail lending and borrowing, the undefined treatment of staking, and the blanket approach to DeFi. The current regulatory framing tends to apply a one-size-fits-all approach, as highlighted in paragraphs 7.4 to 7.10 of the Discussion Paper. This framing assumes that all cryptoasset-related risks are homogenous across the ecosystem, disregarding the nuanced differences between centralised custodial services and decentralised, protocol-governed systems. It conflates technological neutrality with regulatory symmetry—imposing identical compliance burdens on fundamentally different models—and risks flattening two distinct paradigms into a single, misaligned regime. The vast majority of consumer harm to date has stemmed from failures in centralised custodial platforms involving opaque leverage, discretionary management, and poor governance. These are not inherent to the design of decentralised systems. Furthermore, we respectfully disagree with the notion that UK cryptoasset users lack sophistication to warrant a ban on certain services. A recent study by Adan and Deloitte found that the UK, alongside Italy, demonstrated the highest crypto awareness (95%) among the surveyed countries.[1] In our experience, DeFi protocols, including lending and borrowing tools, are primarily used by very capable, sophisticated users that are well aware of the opportunities and the associated risks involved.

Rather than attempting to fit decentralised and non-custodial services into frameworks designed for centralised entities, we respectfully recommend that the FCA consider a bespoke regulatory approach that acknowledges the inherent technical safeguards, public transparency, and permissionless operation offered by non-custodial, onchain operations, such as non-custodial staking and DeFi. Non-custodial models and decentralised

[1] Adan, Web3 & Crypto in France and Europe, 2025

infrastructures should not be treated under the same rules as custodial and centralised services. DeFi is not simply a replication of TradFi on-chain; it is a fundamentally new architecture that embeds transparency, auditability, and automation directly into its protocols. Applying the same rulebook designed for custodial intermediaries, risks making compliance structurally impossible for permissionless systems. Instead, iterative guidance, developed in collaboration with industry stakeholders, is better suited to reflect the diverse risk models and governance structures found across DeFi, staking, borrowing and lending activities.

To truly establish the UK as an internationally competitive hub for cryptoasset services, we, as members of the industry, believe a forward-looking and nuanced regulatory framework is essential – one that champions decentralised and innovative technological solutions. We respectfully suggest that the FCA consider adopting a tiered approach to regulating the crypto market. This would involve tailoring compliance obligations based on the nature and scale of the cryptoasset activity, ensuring that startups and smaller, non-custodial decentralised projects are not overly burdened with compliance obligations designed for larger, centralised financial institutions. Such a differentiated approach would not only mitigate the risk of stifling innovation but also ensure that regulatory efforts are proportionate to the actual risks presented by different models. Imposing overly restrictive rules, originally designed for traditional, centralised financial services, would not only disadvantage users in the UK but also critically undermine the UK's potential in this rapidly evolving market.

IOTA Foundation

DocuSigned by:
Anja Raden
C11470B4DA0E453...

Dr. Anja Raden
Board Member

INATBA

Signed by:
Izzat-Begum B. Rajan
77ADA5F1DB404D3...

Izzat-Begum B. Rajan
Board Chair and Co-Chair of the Finance WG

INATBA

Signed by:
Jean-Christophe Mathonet
88FD5FF141514C2...

Jean-Christophe Mathonet
Co-Chair of the Finance WG

Cardano Foundation

Signed by:
Simone Schürch
06C6847256EA4D9...

Simone Schürch
Senior Legal Counsel

Chapter 2 – Cryptoasset Trading Platforms Question

Question 1: What are the operational and practical challenges of applying the suggested trading, market abuse, and other requirements to authorised overseas firms operating branches in the UK? Are there alternative approaches that could equally mitigate the risks?

The main challenge lies in the FCA expecting full application of UK-specific trading and market abuse rules to firms whose core operations, infrastructure, and compliance frameworks are governed by non-UK jurisdictions. These firms may already be complying with robust standards set by their home regulators, and duplicating compliance for UK purposes—especially in areas like market surveillance, reporting formats, or governance procedures—can introduce unnecessary complexity and cost without meaningfully reducing risk. Instead of imposing a full replication of UK rules, the FCA could adopt a pragmatic home/host cooperation model: apply key UK conduct requirements locally through the UK branch (such as consumer protection and fair trading), while relying on the home supervisor for prudential oversight and technical systems governance, provided there is a formal cooperation agreement in place. This would ensure effective supervision while maintaining the UK's openness to international participation and liquidity.

While extending UK trading and market abuse requirements to overseas branches enhances regulatory consistency and investor protection, they imposes significant operational and legal burdens. A nuanced approach that recognises the regulatory frameworks of home jurisdictions and the business model of branches—backed by strong supervisory cooperation—can achieve the desired outcomes without unnecessary duplication or cost.

Question 2: What are the challenges and limitations of requiring the establishment of an affiliated legal entity for retail access to trading services by an overseas firm with a UK branch?

We support the requirement to have a UK-authorised entity for retail-facing services as it can ensure that retail clients are protected under local supervision. However, this should not escalate into requiring CATPs to replicate all operational activities in the UK as well as abroad. A lean, compliant UK subsidiary for onboarding, KYC/AML, and customer support could suffice, while core trading operations remain with the overseas parent or branch. This structure balances oversight with operational efficiency and avoids deterring high-quality international platforms from engaging with the UK market.

While requiring an affiliated UK legal entity can enhance regulatory clarity and consumer protection, it comes with significant costs, operational burdens, and potential market drawbacks, particularly around competition, innovation, and cross-border efficiency. Alternative approaches—especially those that focus on regulatory outcomes rather than legal form—could offer a more proportionate response.

Question 3: What conditions should apply to the direct access of trading services of an overseas CATP with a UK branch?

We recommend that the UK adopt a regulatory equivalence approach for overseas CATPs operating through a UK branch. Compliance with EU or other equivalent regulatory regimes should be considered sufficient for direct access, provided there is a robust framework for regulatory information exchange or a legal obligation to supply relevant compliance data upon request. This would promote cross-border efficiency while maintaining supervisory integrity. However, exceptions should apply in specific areas where material divergence exists—particularly in AML/KYC standards—to ensure UK-specific consumer protection and financial crime prevention goals are met.

Question 4: What, if any, additional responsibilities should we consider for CATPs, to address the risks from direct retail access?

To address the risks stemming from direct retail access, CATPs should be held responsible for ensuring that retail participants engage with the platform in a way that upholds market integrity, fairness, and transparency. While we strongly support maintaining direct retail access as a distinguishing and innovation-enabling feature of crypto markets, it is reasonable to expect CATPs to implement effective systems to monitor retail behavior, detect potential abuse, money laundering and terrorism financing and maintain clear lines of accountability. Responsibilities such as enforcing platform rules, monitoring for manipulation, and being able to suspend or revoke access in the event of misconduct are appropriate measures to safeguard the market without erecting unnecessary barriers for retail participation.

However, these responsibilities must remain proportionate and aligned with the realities of how crypto-native platforms operate. Traditional financial institutions already deploy a variety of tools to monitor activity and prevent abuse. CATPs should be expected to implement equivalent—not excessive—measures to ensure a level playing field. In fact, crypto platforms are often built on more agile and modern infrastructure, free from legacy system constraints, making it easier to implement real-time surveillance, account-level controls, and automated risk management tools. The goal should be to adapt existing safeguards—not to overburden innovation—with expectations that reflect the technological strengths and operational models of decentralised environments.

Question 5: How can CATPs manage the risks from algorithmic and automated trading strategies?

Algorithmic and automated trading strategies do introduce risks—such as volatility spikes, manipulation, or system abuse—but these risks can be effectively managed without resorting to overly rigid or burdensome requirements. CATPs operate within an environment that is structurally different from traditional financial markets, and any regulatory approach should reflect this difference while still aiming to uphold market integrity.

Rather than assuming crypto platforms require stricter treatment, CATPs should be expected to implement clear, baseline safeguards, such as monitoring for abusive trading patterns,

setting message traffic limits, and flagging suspicious behaviors. This promotes a level playing field without overcorrecting based on perceptions of the crypto sector.

It is also important to recognise that many CATPs offer open access, allowing individual retail users to deploy algorithmic tools independently. Because of this, imposing gatekeeping or pre-authorisation regimes similar to those under MiFID RTS 6 or 8 would be impractical and misaligned with the open nature of crypto markets. A more productive approach would be to require CATPs to adopt general governance and oversight principles, apply relevant monitoring tools, and support transparency, while allowing implementation flexibility according to the platform's design and user base.

Question 6: Do you agree that CATPs should have contractual agreements in place with legal entities operating market making strategies on their platforms? Are there alternative approaches that could equally mitigate the possible risks to market integrity?

We caution against imposing a blanket requirement for CATPs to maintain formal contractual agreements with all legal entities operating market making strategies on their platforms. While transparency and accountability in market making arrangements are important to safeguard market integrity, mandating contractual agreements as the default regulatory approach may introduce unnecessary compliance burdens—especially for DeFi platforms facilitating permissionless or global access, where market makers may be decentralised or pseudonymous. As we explain below (see Question 50), applying the same regulatory framework for both CATPs and decentralised exchanges is not feasible and it creates friction.

In many cryptoasset markets, market making is not performed by a small group of institutions but by a diverse array of participants, including independent liquidity providers and decentralised actors. Enforcing contractual obligations in such a setting risks undermining the open and borderless nature of these markets. A more innovation-friendly approach would be to encourage platforms to clearly disclose whether affiliated or incentivised market makers operate on the platform, publish the terms of any incentive programs (such as rebates or volume tiers), and implement monitoring mechanisms to identify manipulative practices like wash trading or spoofing.

Nevertheless, contractual agreements between centralised CATPs and professional, incorporated market makers can be a sensible, enforceable, and structured approach to promoting market integrity. However, such requirements may not be feasible in a DeFi context. Given the crypto industry's technological decentralisation, pseudonymity, and global access, the regulatory approach should be nuanced.

Question 7: Is there a case for permitting discretionary trading practices for CATP operators? If so, how could the above risks be appropriately mitigated?

There is a case to be made for permitting limited discretionary trading practices on CATPs, particularly in niche or low-liquidity markets where rigid non-discretionary systems may hinder effective execution or price discovery. Cryptoasset markets are not monolithic; while

many operate efficiently with automated order books, some emerging tokens or institutional trading strategies may benefit from a more tailored, discretionary execution approach—especially where execution needs cannot be met through purely algorithmic matching. To outright ban discretionary trading may risk oversimplifying market structure and removing tools that, when properly governed, can serve legitimate use cases.

That said, the risks of discriminatory behavior or opaque execution must be addressed if discretion is allowed. Any such permissions should be narrowly defined, limited to specific circumstances (such as OTC-style execution or low-liquidity pairs), and paired with clear transparency obligations and governance standards. CATPs should be required to disclose the conditions under which discretion is used, apply consistent internal rules for decision-making, maintain audit trails, and regularly report the volume of transactions executed under discretionary arrangements. This aligns with the broader recommendation in the INATBA's DeFi Self-Regulation proposal, reinforcing accountability and helping to ensure that discretionary trading does not become a channel for preferential treatment or abuse. This would preserve market fairness while allowing platforms the operational flexibility to serve different types of market participants and asset types without resorting to rigid traditional market models that don't fit crypto's unique dynamics.[2]

Question 8: Should firms operating a CATP be permitted to execute transactions on a matched-principal basis? If so, how could the above risks be appropriately mitigated?

Yes, firms operating a CATP should be permitted to execute transactions on a matched-principal basis, provided that appropriate guardrails are in place. Matched principal trading (MPT) is a common and well-understood model in traditional finance, especially for facilitating efficient execution and managing liquidity across fragmented markets. A blanket prohibition could restrict legitimate business models, discourage market making, and potentially hinder innovation in execution mechanisms that may serve both institutional and retail participants effectively.

The key risk here is not the MPT model itself, but a lack of transparency or inadequate conflict-of-interest management. These risks can be mitigated through clear disclosure of when MPT is used, full auditability of trade execution, and robust governance arrangements that separate execution logic from proprietary trading strategies. Additionally, matched principal trades should be subject to best execution rules and pricing benchmarks, ensuring that they result in outcomes at least as fair as agency-based executions.

Question 9: Have we properly identified the risks from the operator of a CATP also being able to deal in principal capacity off -platform? What is your view on these risks and whether it should be permitted or restricted for an operator of a CATP? If permitted, how should those risks be mitigated?

The risks identified in the discussion paper regarding CATP operators dealing in principal capacity off-platform are broadly understood, but the current framing arguably overstates their potential impact and underestimates the feasibility of mitigation through proportionate

[2] INATBA, DeFi Self-Regulation Proposal, 2025.

measures. The assumption that all off-platform principal activity inherently creates unacceptable conflicts of interest ignores both the operational reality of crypto markets and the capacity of firms to manage such risks through structural separation and disclosure mechanisms.

Rather than imposing blanket restrictions, the more pragmatic and innovation-friendly approach would be to permit off-platform principal trading under specific conditions. These could include clear and auditable separation between trading and CATP operations (either operational or legal), comprehensive disclosure to clients and regulators about any affiliations or potential conflicts, robust internal controls and transparency regarding execution pricing when CATPs interact with affiliated entities. Just as traditional financial institutions are permitted to operate across multiple functions with proper safeguards in place, crypto firms should be afforded similar flexibility provided that they meet clearly defined transparency and governance standards.

Question 10: What are the risks from an entity affiliated with the CATP trading in principal capacity either on the CATP or off the CATP? What additional requirements are necessary to mitigate these risks?

The key risks stem from information asymmetries, preferential treatment, and the perception—or reality—of rigged markets. If a CATP-affiliated trading firm has advanced knowledge of order flows, execution timing, or platform decisions, it holds an unfair advantage over other participants. This can drive away legitimate liquidity providers and discourage retail participation, undermining the long-term health of the market.

To mitigate these risks, regulatory frameworks should mandate legal separation, independent governance, and disclosure of trading relationships between the CATP and its affiliates. Functional separation should go beyond paper firewalls—it should include restricted access to sensitive platform data, independent audits, and an obligation to maintain equivalent latency and access conditions for all trading participants. A further requirement could be a cap on the volume or market share of trading activity that affiliated entities can conduct on the platform, to prevent overreliance on internal liquidity and ensure a healthy degree of external participation.

Question 11: What are the risks from admitting a cryptoasset to a CATP that has material direct or indirect interests in it? How should we address these?

The primary risk of admitting a cryptoasset to a CATP in which the platform has a material direct or indirect interest lies in the potential for serious conflicts of interest. If the CATP stands to benefit financially from the success or trading activity of the asset, it may be incentivised to give that asset preferential treatment—through increased visibility, more favourable liquidity arrangements, or even through abusive practices such as wash trading or selective listing criteria. This undermines market integrity and creates an unlevel playing field for other issuers. It can also mislead retail investors, who may not be aware of the platform's commercial ties to the asset and may assume the listing itself constitutes a form of endorsement or due diligence.

Rather than impose blanket prohibitions, a more proportionate response would be to require legal or functional separation between the CATP operator and any affiliated issuer. Additional obligations should include mandatory disclosures of all material interests, transparent listing criteria, and limitations on the trading activity of affiliated entities to prevent manipulation. Regulatory oversight should also ensure that CATPs with such interests implement strict internal controls and provide adequate audit trails. This approach allows the market to benefit from innovation and vertical integration without compromising fairness or trust.

Question 12: Are there important reasons why the same entity authorised to operate a CATP should also be able to provide credit lines or financial accommodations to the CATP's clients?

Yes, there are several important reasons why the same entity authorised to operate a CATP should be allowed to provide credit lines or financial accommodations to its clients, particularly in the context of fostering healthy market activity, ensuring global competitiveness, and adapting to the operational realities of digital asset markets.

First, access to credit lines and financing mechanisms is a critical liquidity enabler for professional market participants, including market makers and institutional traders. Denying CATPs the ability to offer such facilities—when done transparently and with adequate risk controls—could impair liquidity provision on the platform and disincentivise participation from capital-efficient players. Many jurisdictions currently allow such accommodations, including for traditional models, under proper oversight, and imposing a UK-specific prohibition would likely disadvantage domestic platforms relative to their international peers.

Second, CATPs are often best positioned to assess the trading behavior and risk profile of their clients, given their real-time access to data on order activity and historical performance. This can allow them to tailor risk-managed credit offerings far more effectively than disconnected third-party providers. With appropriate safeguards in place—such as disclosure of credit terms, limits based on objective metrics, and internal firewalls between trading and risk teams—these accommodations can be responsibly managed.

Rather than prohibit such services, the more proportionate approach would be to regulate the terms under which they are offered. This could include requiring full disclosure to clients, transparent risk management practices, and a clear distinction between collateralised and uncollateralised facilities. In our opinion, it can be appropriate and efficient for the same authorised CATP operator to provide credit lines or financial accommodation, provided strong governance, risk management, and regulatory safeguards are in place. This helps balance client service benefits with market integrity and financial stability.

Question 13: Do you agree with our proposal to prevent CATPs from managing or internalising credit risks between counterparties trading on their platforms? If not, why not and how would you suggest the CATP manage these risks?

We do not support a full prohibition on CATPs managing or internalising credit risk between counterparties. While we recognise the FCA's aim to limit systemic risk and preserve market

neutrality, we believe there are circumstances under which such credit risk management—if properly disclosed and tightly governed—can enhance platform resilience and market efficiency. A more proportionate, risk-based approach would be preferable to a blanket restriction, particularly given the current structure and operational needs of crypto markets.

In the absence of mature clearing infrastructure or external credit risk intermediaries in crypto markets, many CATPs have filled this gap by facilitating settlement, managing margin requirements, or internalising limited credit risk. These functions—especially in high-frequency or 24/7 environments—are essential for timely execution and efficient market functioning. Prohibiting CATPs from managing these exposures may reduce their ability to support deep, liquid markets and could drive activity to less transparent offshore venues.

Instead of hard restrictions, a risk-based framework should be introduced. CATPs should be allowed to manage counterparty credit exposures provided they have robust capital buffers, automated risk management systems (e.g. real-time collateral monitoring), and transparent internal policies for margin calls, liquidations, and loss socialisation mechanisms (if applicable). Similar approaches have worked well in traditional finance through prime brokerage services and central clearing mechanisms. In other words, CATPs should focus on robust margining, risk controls, and leveraging authorised CCPs or clearing services.

The FCA should also consider that some CATPs may wish to evolve toward hybrid models—combining execution and clearing—which can improve settlement efficiency and mitigate systemic risks if designed appropriately. Rather than forcing all credit risk management outside the platform, the regulator should establish minimum governance, disclosure, and prudential requirements for those CATPs who choose to manage credit exposures in-house. This would better reflect the decentralised and rapidly evolving nature of the industry without compromising on systemic safety.

Question 14: How should we interpret or define settlement for the purpose of CATP settlement rules? Would these rules be specific to CATPs or should they be extended to other trading activities?

Settlement, in the context of CATPs, should be interpreted as the point at which the legal and practical transfer of a cryptoasset between buyer and seller becomes irrevocable and final, in accordance with the terms agreed at the time of trade execution. Given the distinct nature of cryptoasset transactions settlement may not always correspond to a single moment in time but rather to the completion of a verifiable, irreversible transfer of control over the cryptoasset. For regulatory purposes, settlement rules should initially be specific to CATPs, given their role in internalising settlement processes and managing custody functions for users. Applying traditional settlement frameworks designed for intermediated, multi-layered financial systems would be inappropriate and potentially burdensome.

Question 15: Do you agree that CATPs should be subject to both pre-trade and post-trade transparency requirements? Are there any reasons we should consider pre-trade transparency waivers?

We support the principle of enhancing transparency in cryptoasset markets, but we recommend caution in applying blanket pre-trade and post-trade transparency requirements to all CATPs without accounting for the nuances of market structure, asset liquidity, and participant profiles.

CATPs should be subject to both pre-trade and post-trade transparency requirements, as these are critical to ensuring fair, efficient, and orderly markets, particularly as retail and institutional participation in crypto grows. However, limited pre-trade transparency waivers may be justified under certain conditions to protect market functioning and liquidity.

Pre-trade transparency, in particular, can introduce significant challenges for CATPs, especially those listing low-liquidity tokens or facilitating institutional trading strategies that depend on some degree of execution discretion. Publicly displaying full depth-of-book or large orders in real-time could lead to front-running, reduce the willingness of liquidity providers to post firm quotes, and ultimately harm price discovery rather than enhance it. In traditional markets, transparency waivers are permitted in certain cases (e.g. block trades or illiquid instruments), and we believe a similar, calibrated waiver system should be developed for crypto markets.

We recommend allowing CATPs to apply for pre-trade transparency waivers based on objective criteria—such as token liquidity, trading volume, average spread, or order size. Such a system would encourage responsible market-making without disproportionately harming liquidity providers or fragmenting the UK crypto market. Moreover, pre-trade transparency should not be seen as a one-size-fits-all solution: aggregated order book snapshots, time-lagged data, or tiered disclosure frameworks could achieve regulatory goals while still protecting market functionality.

Post-trade transparency, by contrast, should be required—but with allowances for short deferrals (especially for large trades) and protection of counterparty identity. To that end, we support the introduction of standardised formats for publishing trade data and ask that the FCA engage with industry to co-develop such standards.

Question 16: Which challenges may emerge for transaction data requirements if there is direct retail participation?

In our opinion, handling of transaction data includes several challenges for the collection, quality, and utility of transaction data. To maintain fair and orderly markets, transaction data regimes must evolve to reflect the retail-intensive and high-volume nature of cryptoasset trading. Furthermore, in the area of decentralised finance, transaction data already exists on chain and it is not feasible to require decentralised finance protocols to comply with client-facing obligations.

Question 17: Are there preferred standards for recording transaction data?

Preferred standards for recording transaction data in the cryptoasset space should aim for interoperability with existing regulatory reporting frameworks while accounting for crypto-specific characteristics. From a regulatory consistency standpoint, ISO 20022—already

widely adopted in traditional finance—offers a useful foundation for structuring transaction metadata in a machine-readable, scalable way. Similarly, the FSB's and IOSCO's work on cryptoasset data reporting provides early-stage direction for harmonising definitions and schemas. A hybrid approach may be most appropriate, where off-chain records mirror key on-chain events in standardized formats and are reconciled through cryptographic proofs or APIs. This avoids over-reliance on any one infrastructure layer and enables smoother interoperability across CATPs, custodians, and regulators.

Question 18: What opportunities and challenges do you see in trying to harmonise on-chain and off-chain transactions' recording and/or reporting?

Harmonising on-chain and off-chain transaction records presents an opportunity to establish a more resilient and transparent market infrastructure, something traditional finance has long struggled to achieve. When done correctly, on-chain recording can serve as a publicly verifiable audit trail, reduce information asymmetries, and simplify regulatory access to transaction data. It can also improve dispute resolution, increase the traceability of market abuse, and streamline cross-border regulatory cooperation.

Data on public blockchains is publicly available. Although on-chain data often lacks meaningful attribution to individual participants unless combined with off-chain identity layers, the data is permanent and immutable, meaning that historical on-chain data could be linked back to an individual if the personal attributes are revealed or leaked at any point. The fragmentation of protocols and differing data structures across chains also makes standardisation difficult. Not all CATPs use the same infrastructure, and some use proprietary ledgers or off-chain matching engines, further complicating harmonisation efforts.

Finally, authorities (e.g., the FCA or HM Treasury) should consider leading the development of a harmonised crypto transaction reporting framework with: i) a standardised data dictionary for on/off-chain events; ii) required wallet-to-user traceability for regulated venues; iii) and phased implementation through regulatory sandboxes.

Chapter 3 – Cryptoasset Intermediaries

Question 19: What practical challenges might firms face if they are required to comply with these order handling and best execution requirements? Are there any alternative approaches that would deliver the same or better order execution outcomes for retail and non-retail customers respectively? Please explain why they may be preferable.

Implementing best execution standards in the fragmented crypto market will present several practical hurdles, particularly for smaller intermediaries. Unlike traditional finance, where price discovery is relatively centralised, crypto markets operate across dozens of venues with significant pricing divergence and liquidity fragmentation. Continuously monitoring prices across multiple exchanges, factoring in not only price but also gas fees, slippage, and latency,

requires robust infrastructure that many firms—especially retail-facing ones—may not currently possess.

Another challenge lies in defining what constitutes “best execution” in environments where the same asset can vary significantly in price from one second to the next due to low liquidity or high volatility. For firms acting on a principal basis, balancing best execution obligations with their own exposure management may prove operationally complex.

An alternative worth exploring is a principles-based approach, focused on core metrics such as price, cost of execution, and speed, which could provide firms with the flexibility to tailor algorithms and infrastructure according to their specific operating models. This would maintain the regulatory goal of ensuring fair outcomes without imposing undue technical burdens, particularly on smaller or less-resourced firms.

Question 20: What benefits and risks do you see with the proposed guidance requiring firms to check the pricing for an order across at least 3 UK-authorised trading platforms (where available)?

The proposed guidance requiring firms to check pricing for an order across at least three UK-authorised trading platforms is well-intentioned in its aim to promote best execution and fair pricing for retail customers. However, its practical implementation raises several concerns. While encouraging broader price discovery is generally positive, mandating a strict minimum number of venues risks creating unnecessary friction—especially in a nascent and fragmented market like crypto. Small firms are unlikely to be able to comply due to the high initial implementation costs.

Many cryptoassets may only be listed on one or two UK-authorised platforms, particularly in the early stages of their market adoption. Imposing a three-platform requirement in such cases could either force firms to deny execution altogether or push them to use indirect and less efficient pricing proxies, which may not reflect real-time market conditions. This can lead to reduced market access for both firms and consumers, and paradoxically may harm the very execution quality the rule aims to protect.

Moreover, constantly polling multiple venues for each transaction may impose a significant infrastructure and latency burden, especially for smaller firms without institutional-grade systems. Over time, such a requirement could lead to market consolidation by disadvantaging smaller or newer entrants who cannot meet the technical demands, ultimately reducing competition and consumer choice.

A more innovation-aligned approach would be to encourage pricing checks across multiple venues where reasonably possible but avoid setting a hard minimum. Firms could instead be required to demonstrate the effectiveness of their pricing methodology and show that it achieves fair execution outcomes, rather than relying on a rigid numeric benchmark.

In this light, you will possibly allow firms to use trusted price aggregators or market data providers that consolidate prices from multiple venues to reduce latency and complexity. Permit sampling or periodic checks rather than per-trade checks to balance execution speed

and quality. And also introducing exceptions for tokens with low venue coverage or extreme volatility.

Question 21: What benefits and risks do you see with the idea that best possible results should be determined in terms of the total consideration when firms deal with retail customers?

Determining best possible results in terms of total consideration—meaning the combined cost of the cryptoasset's execution price and all related fees (such as platform fees, settlement costs, and gas fees)—is an essential and practical standard for safeguarding retail investors in crypto markets. This approach reflects the realities of fragmented liquidity and varied execution methods across platforms, where an asset may appear cheaper in price but ultimately be more expensive once all hidden or opaque charges are included. By focusing on the total economic impact of a trade, rather than just the headline price, this rule provides a transparent and objective benchmark that aligns with the FCA's Consumer Duty and pushes intermediaries to act in the genuine best interest of their clients.

At the same time, the application of this standard presents practical challenges. Crypto markets often lack standardisation in fee disclosure, and intermediaries may use different pricing structures—bundled spreads, tiered gas fees, or dynamic pricing models that are not always clearly visible to end-users. Moreover, retail clients may not have the tools or access to verify whether they received the best total consideration, making firms' record-keeping and disclosure obligations especially critical. To ensure that the standard is meaningful in practice, clear regulatory guidance on cost breakdowns, methodologies for calculating total consideration, and periodic audits or reviews would be essential.

In our opinion, using total consideration as the benchmark for best execution with retail clients improves transparency and aligns incentives towards truly cost-effective execution. However, it requires clear, standardised cost disclosures and flexibility to accommodate variable fees and market conditions.

Question 22: Do you see any potential problems with the proposal to restrict intermediaries to offering regulated services for UK retail customers solely for crypto assets admitted to trading on a UK authorised CATP?

The proposal to restrict intermediaries to offering services only for cryptoassets admitted to trading on a UK-authorised CATP makes sense from a regulatory coherence standpoint and reflects an effort to anchor consumer protection within a supervised market structure. We understand the rationale: it ensures that retail clients interact only with assets that meet a minimum threshold of oversight, mitigating risks around transparency, fraud, and manipulation. In principle, this direction contributes to building trust in the market and creates a clearer accountability framework for retail-facing firms.

Still, this approach raises concerns around its practical effects on innovation. The vast majority of cryptoasset activity—particularly early-stage, experimental, or emerging use cases—occurs in ecosystems that have not yet sought admission to UK-authorised trading venues.

Restricting access exclusively to admitted assets could effectively exclude retail users from participating in the formative stages of innovation, while reinforcing the position of a few gatekeepers who determine which assets get admitted. This creates bottlenecks, dampens competitive dynamics, and limits exposure to the full spectrum of technological development occurring in crypto markets globally.

The direction may be right, but it risks being too rigid. If pursued, the framework should include some pathway for responsibly onboarding cryptoassets that are not (yet) admitted to a UK CATP—perhaps through enhanced disclosure, risk warnings, or thresholds based on liquidity, market cap, or user adoption. Without that, the rule risks not only stifling innovation but also creating a distorted market where retail users are boxed into a narrow set of assets, while the real activity continues offshore, out of sight, and out of reach.

Some balanced approaches that can help protect UK retail investors while preserving market access and innovation include introducing a tiered listing regime or a secondary category of "provisionally eligible" cryptoassets. These could be accompanied by enhanced disclosure obligations, risk warnings, and activity limits. This would allow intermediaries to offer access to emerging tokens in a controlled, transparent manner while avoiding complete exclusion from innovation pipelines that have not yet passed through formal CATP admission processes.

Question 23: Are there any specific activities or types of transactions we should expressly carve out of our proposed order handling and best execution rules? If so, why?

Yes, certain activities and transactions may warrant carve-outs from strict order handling and best execution rules to ensure operational feasibility without undermining market integrity. For example, large block trades, or trades involving highly illiquid cryptoassets may not lend themselves well to real-time best execution benchmarks due to the risk of significant price impact or front-running. In these cases, rigid adherence to standard execution protocols could discourage participation or distort execution quality. Carve-outs should therefore be permitted under narrowly defined conditions—such as minimum trade size thresholds or designated liquidity classifications—paired with enhanced disclosure and post-trade transparency obligations to mitigate risks.

Question 24: What risks arise when specific instructions (for example, specifying which execution venue to use) from retail customers are allowed to override certain best execution requirements? How can these be mitigated?

Allowing retail customers to override best execution requirements by specifying particular execution venues introduces a fundamental tension between respecting user autonomy and ensuring investor protection. The primary risk is that customers may lack the technical or market knowledge to assess the relative quality or reliability of different execution venues. They may be influenced by brand recognition, social media narratives, or misinformation, leading them to choose venues with poor liquidity, high slippage, or opaque fee structures. This could result in demonstrably worse execution outcomes than if the intermediary had exercised discretion under a best execution framework. Additionally, there is a danger that

firms could use the "client instruction" loophole to shift responsibility away from themselves and avoid their best execution obligations.

That said, user-directed execution is also an important feature in an increasingly sophisticated market environment. Many crypto users are well-informed and may wish to interact with specific venues due to product availability, technical integrations, or personal preference. To mitigate the risks, firms should be required to provide a clear, concise explanation of the potential implications of overriding best execution—particularly when the client's choice may lead to suboptimal pricing or higher fees. They should also document the instruction and, where appropriate, offer real-time comparisons or warnings if the chosen venue significantly deviates from market benchmarks.

Question 25: Are there circumstances under which legal separation should be required to address potential conflicts between executing own orders and client orders?

Legal separation may be appropriate in circumstances where a firm simultaneously engages in proprietary trading and client order execution on the same platform, particularly if the firm has privileged access to order flow information or internalises client trades. In such cases, structural separation can help mitigate conflicts of interest, promote transparency, and ensure fair treatment of clients. Legal separation should be required when conflicts are significant and cannot be effectively managed by internal controls alone. It is especially important to preserve market integrity and client trust. However, these requirements should be proportionate to the scale and complexity of the business—meaning smaller or innovative firms may not require full legal separation but must still meet clearly defined minimum safeguards. At the very least, firms should be required to prohibit front-running, disclose their own trading activity clearly, and implement auditable best execution policies. Proportionality should not mean exemption from basic conflict-of-interest protections, but rather a flexible framework for how those protections are implemented.

Question 26: Are there any other activities that may create conflicts of interest and risks to clients if performed by the same intermediary? How can these be managed?

Yes, several additional activities may create significant conflicts of interest when performed by the same intermediary. One such activity is acting as both a market maker and a broker for retail clients. In these dual roles, a firm may be incentivised to prioritise liquidity provision or inventory management over securing the best execution for client trades, especially in less liquid markets. Another example is when intermediaries simultaneously offer custodial services and operate trading platforms. This vertical integration can create risks around front-running, unfair access to user data, or even using custodial assets in ways that are not in the client’s best interest, particularly if not subject to clear functional separation or oversight.

These risks can be managed through a combination of transparency, operational safeguards, and regulatory oversight. Functional separation between roles, with distinct teams, systems, and decision-making processes can help reduce internal conflicts. Firms should also be required to disclose the nature of their activities clearly, so clients are fully informed of potential conflicts. Where structural separation is not viable, strong internal governance,

regular conflict of interest assessments, and external audits can be appropriate mitigants. Importantly, a one-size-fits-all regulation proved to often be inadequate in traditional models and should not be repeated in the crypto-assets market. A more tailored, proportionate regime that incentivises transparency and good-faith risk management would be a more effective and innovation-friendly solution.

Question 27: What benefits does pre-trade transparency provide for different types of market participants and in what form will it be most useful for them? Please provide an analysis of the expected costs to firms for each option if available.

Pre-trade transparency can offer clear benefits to different categories of market participants in the cryptoasset ecosystem. For retail customers, it increases access to timely pricing information, helping them better assess execution quality and make more informed trading decisions—particularly important given the fragmented nature of crypto markets and the absence of consolidated order books. For institutional participants and intermediaries, enhanced transparency supports more accurate risk pricing, better execution benchmarking, and can ultimately drive healthier competition across trading venues. Where indicative or firm quotes are made available, especially for various trade sizes, intermediaries are better equipped to serve client orders with clarity and confidence. This, in turn, can reduce information asymmetries and foster greater market integrity.

That said, imposing broad and rigid pre-trade transparency obligations—such as mandatory quote publication or firm pricing for all assets and order sizes—could carry unintended costs and/or externalities. Requiring real-time quote dissemination across all trades could discourage liquidity provision, particularly for less liquid or newly listed cryptoassets. Market makers and intermediaries might be reluctant to show firm prices if they are exposed to predatory trading behavior or forced to reveal sensitive inventory positions. Operationally, smaller firms may also struggle to implement and maintain robust infrastructure to support these disclosures, especially in the absence of consolidated data systems like those in traditional markets. A flexible, proportionate approach—where larger firms and more liquid assets bear a higher obligation, and where exemptions or deferrals apply to protect liquidity—would best balance market transparency with cost and competition considerations.

Question 28: What alternative solutions to the post-trade transparency requirements proposed above could mitigate the risks? Please provide an analysis of the expected costs to firms for each option if available.

One alternative to full real-time post-trade transparency is the implementation of delayed public reporting based on trade characteristics such as size or asset liquidity. For example, large transactions or trades involving low-liquidity cryptoassets could be published with a short delay (e.g., 15–60 minutes), while smaller or highly liquid trades could be reported more quickly (e.g., within 1–5 minutes). This approach balances the need for market transparency with the need to avoid exposing trading strategies or discouraging liquidity provision. Firms would need to invest in systems for timestamping and categorizing trades, but the expected implementation cost would vary depending on firm size.

Question 29: Do you believe that certain cryptoassets should be exempted from transparency requirements? If so, what would be the most appropriate exemption criteria which would best balance the benefits from transparency and costs to the firms?

Yes, certain cryptoassets should be exempted from strict transparency requirements. Illiquid tokens, newly launched assets, or those with very low daily trading volumes are prime candidates for such exemptions. Requiring full pre and post-trade transparency for these assets can lead to unnecessary operational burdens for CATPs without offering material improvements in price discovery or investor protection. Moreover, forcing transparency on thinly traded markets could inadvertently increase volatility or disincentivise listings of innovative tokens. Exemptions should be narrowly tailored and justified by clear criteria. They help balance meaningful transparency with operational feasibility and innovation support. In addition to that, proper safeguards and ongoing oversight are critical to prevent regulatory gaps.

Question 30: What would be the most appropriate exemption threshold to remain proportionate to the size of the firm while balancing the benefits from transparency and costs to the firms?

An appropriate exemption threshold for cryptoasset intermediaries should be based on objective and scalable metrics that reflect the firm's size and market impact. We recommend considering a combination of quantitative criteria such as (i) annual trading volume, (ii) average daily client order flow, and (iii) total assets under custody (if applicable). For instance, firms with less than £50 million in annual notional trading volume, or managing fewer than 10,000 individual retail trades per quarter, could be exempt from full pre and post-trade transparency requirements or be subject to simplified reporting standards. This approach would ensure that the regulatory burden remains proportionate while still incentivising responsible conduct from all participants.

At the same time, exemptions must not compromise the overall goal of improving market transparency and fairness. Tailored thresholds can allow smaller or early-stage firms to innovate and grow without being overburdened by operational and technological requirements designed for larger players. However, such firms should still maintain basic execution records and be prepared to demonstrate fair pricing practices upon request. A tiered compliance structure, whereby firms progressively adopt fuller transparency obligations as they scale, would strike the right balance between safeguarding consumer outcomes and supporting innovation and competition within the UK crypto intermediary landscape.

We believe that in order to set a proportionate exemption threshold that balances transparency benefits with cost burdens—especially for smaller firms—the threshold must consider both firm-level capacity and cryptoasset market relevance. In this light, a tiered, multi-factor exemption approach based on volume, size, and token liquidity offers a balanced, proportionate model. It reduces costs for small firms, preserves transparency where it matters, and is adaptable as markets mature.

Question 31: What are the crypto-specific risks of opting retail customers up? How should these be managed and what additional guidance on how to assess the expertise, knowledge and experience of clients can we give firms to better mitigate risks of harm?

The primary crypto-specific risk of opting retail customers up to professional status lies in the volatility and technical complexity of the market. While many retail clients may have hands-on experience, distinguishing genuine sophistication from exposure alone is difficult. Without careful assessment, some clients may overestimate their understanding and take on risks they aren't equipped to manage, particularly in areas like tokenomics, liquidity fragmentation, or novel trading products.

To mitigate these risks, firms should be required to conduct a rigorous, crypto-specific assessment of each client's experience, knowledge, and expertise. This could include verifying actual trading history across various asset types, understanding of risks specific to tokenomics and custody, and engagement with self-directed research or tools. The FCA should provide practical guidance tailored to crypto, focusing on demonstrated competence rather than legacy financial credentials. This avoids overprotection while ensuring clients who opt up are genuinely equipped.

Question 32: What are the benefits of having quantitative thresholds when opting clients up? How should we determine any quantitative threshold? What alternative rules or guidance specific to crypto should we consider?

Quantitative thresholds such as trade frequency, volume, or portfolio size can offer a useful baseline to support a consistent opt-up process, helping firms identify retail clients with relevant exposure. These thresholds, however, should not be used as blunt instruments. The thresholds should be flexible and assessed in context, recognising that meaningful engagement with the market may occur even without large financial exposure. For instance, a client who has conducted 10–20 trades per quarter across different exchanges and asset types may be more informed than one with a larger portfolio but minimal trading activity.

Quantitative thresholds help standardise and professionalise opt-up processes, but they must reflect crypto's distinct market dynamics. Thresholds should be paired with behavioural and educational assessments and reviewed regularly to ensure proportionality and effectiveness.

Chapter 4 – Cryptoasset lending and borrowing

Question 33: Do you agree with our understanding of the risks from cryptoasset lending and borrowing as outlined above? Are there any additional risks we should consider?

We broadly agree with the FCA's identification of key risks in cryptoasset lending and borrowing but believe it is critical to avoid framing the activity itself as inherently harmful. Crypto lending and borrowing are essential components of the broader crypto market infrastructure. They facilitate liquidity, enable capital efficiency, and offer alternative access to

financial services outside the traditional banking system. The failures that occurred in 2022 were not due to the nature of lending and borrowing, but due to poor governance, lack of transparency, and unsustainable practices by a few decentralised platforms. These events highlighted the importance of adequate risk management and disclosures, not a fundamental flaw in the model.

It is important to distinguish between the risks posed by decentralised entities and the structures emerging in decentralised markets. In decentralised models, the transfer of legal and beneficial ownership can expose users to platform solvency risk and mismanagement. Consumers often do not understand that lending arrangements may treat them as unsecured creditors, particularly when terms are buried in lengthy, non-transparent agreements. The reinvestment of user assets into illiquid positions or the use of affiliated platform tokens to inflate yield exposes users to liquidity risks and conflicts of interest. These practices must be addressed, not through bans on lending activity, but through regulatory requirements for disclosures, segregation of functions, and restrictions on opaque token-based incentives.

In decentralised environments, where lending and borrowing arrangements are governed by transparent code and automated execution, several of these risks can be mitigated. While these models are not risk-free, they offer new ways to manage collateral, execute margin calls, and prevent human interference. However, they also come with their own challenges — such as smart contract vulnerabilities, lack of formal recourse mechanisms, and difficulty in enforcing jurisdictional accountability. These risks are materially different from those in decentralised models and should not be regulated identically. A one-size-fits-all framework would either leave gaps or unintentionally stifle innovation.

We also encourage the FCA to consider the importance of informed consumer participation. It is not feasible to assume all retail consumers lack the capacity to understand crypto lending mechanisms. However, there is a clear need for platforms to provide meaningful, accessible explanations of how yield is generated, the nature of collateral, and what rights (or lack thereof) consumers have in case of default or insolvency. The focus should be on ensuring consumers can make decisions with clarity about the risks, rather than restricting access based on the presumption of incompetence.

Finally, any regulatory framework should be designed to promote resilience and competition in the UK market. Overly restrictive rules could push activity offshore or into less transparent environments, leaving consumers worse off. Conversely, rules that require decentralised platforms to maintain appropriate reserves, manage counterparty risk, and disclose key operational practices can create a safer and more trustworthy lending environment.

Question 34: Do you agree with our current intention to restrict firms from offering access to retail consumers to cryptoasset lending and borrowing products? If not, please explain why.

We respectfully disagree with the current intention to restrict firms from offering access to cryptoasset lending and borrowing products to retail consumers. Such a restriction would

significantly undermine the foundational principles of decentralised finance and stifle innovation in one of the most promising areas of the crypto economy. Crypto lending and borrowing mechanisms are not fringe financial products—they are essential infrastructure that enables decentralised capital formation, liquidity provision, and market efficiency in the absence of traditional financial intermediaries. Removing retail access to these tools effectively negates the value proposition of open financial systems.

DeFi lending protocols, in particular, offer transparent, auditable, and non-custodial alternatives to opaque traditional finance lending models. Unlike centralised lenders that failed due to poor risk management and lack of disclosures, on-chain lending protocols allow users to inspect the health of the system, verify collateralisation levels, and track asset flows in real time. These features do not exist in the traditional financial system, where credit allocation and risk exposure are typically hidden behind institutional walls. Banning these activities for retail users due to failures in centralised actors conflates the risks of permissionless lending protocols with those of off-chain, custodial lending services—two radically different models.

Moreover, limiting access to such products on the basis of perceived consumer vulnerability may create greater harm by driving users toward unregulated offshore platforms that lack even minimal oversight. Retail users seeking yield will continue to participate in crypto lending, whether domestically or abroad. A restrictive regime risks externalising those risks rather than managing them within a regulated perimeter. A more constructive approach would focus on targeted safeguards such as robust disclosure obligations, and caps on leverage or collateral concentration, rather than blanket prohibitions.

It is also important to recognise that cryptoasset lending is not a homogenous activity. Protocols differ in terms of how they manage collateral, automate liquidations, or distribute yield. Treating all models as inherently unsuitable for retail users ignores the diversity of designs and the ongoing evolution of risk management practices within the sector. The UK should be aiming to lead in shaping high-integrity DeFi rather than excluding consumers from it.

Crypto lending and borrowing are not speculative side products—they are core pillars of the emerging digital financial architecture. A forward-looking regulatory regime should recognise this and seek to enable responsible retail participation rather than shutting it down wholesale. We encourage the FCA to consider more nuanced approaches that distinguish between centralised custodial models and decentralised non-custodial protocols, and to work collaboratively with the industry to establish proportionate consumer protection mechanisms that do not undermine the integrity of open financial systems.

Question 35: Do you agree that applying creditworthiness, and arrears and forbearance rules (as outlined in CONC) can reduce the risk profile for retail consumers? Could these be practicably applied to existing business models? Are there are any suitable alternatives?

We do not agree that applying the creditworthiness and arrears/forbearance rules from CONC to cryptoasset borrowing would be appropriate or effective. These rules are designed

for unsecured fiat-based consumer credit arrangements in traditional finance, not for overcollateralised, on-chain lending where credit risk is already substantially mitigated by the use of smart contracts, liquidation mechanisms, and real-time market pricing.

In cryptoasset borrowing, the collateralisation ratios—often exceeding 150%—serve as the primary consumer protection mechanism. The system is not reliant on a borrower's credit history, income verification, or affordability checks, but rather on the objective value of the collateral, continuously updated via oracles. Applying affordability assessments in this context misunderstands the fundamental risk model of DeFi borrowing: there is no risk to the lender of not being repaid because the assets to cover the loan are already locked in a smart contract. It also misunderstands the user base. Many participants do not borrow for consumption, but rather for liquidity management, hedging, or arbitrage strategies. The regulatory framing borrowed from traditional consumer credit wrongly assumes the intent and mechanics of crypto borrowing are analogous to payday loans or credit card debt.

Furthermore, most crypto borrowing platforms operate non-custodially and without discretionary intervention. There is no manual process by which a platform would evaluate personal data to conduct a creditworthiness assessment, nor would it be technologically feasible in a decentralised environment where pseudonymity is the default. Applying these rules would effectively require DeFi protocols to centralise operations and KYC their users, defeating the very design goals of the architecture and excluding UK users from global permissionless markets.

As for arrears and forbearance, these are simply inapplicable in systems where loans are automatically liquidated according to predefined smart contract logic when the loan-to-value threshold is breached. There is no concept of being "in arrears" if repayment is enforced via the collateral. Introducing mandatory forbearance periods or manual intervention points would delay liquidation and increase systemic risk for the protocol and its users. In the context of volatile assets, this would likely lead to greater losses for both borrowers and lenders.

Instead of misapplying inappropriate legacy frameworks, regulators should focus on improving transparency, standardising disclosures about collateral risks, and ensuring that retail borrowers are informed—via enforced pre-contractual disclosures and risk flags—about the implications of price volatility, automatic liquidations, and collateral ownership. Smart contract code audits, public documentation of parameters (e.g., collateralisation ratios, liquidation penalties), and accessible simulation tools for retail users would be far more meaningful than attempting to retroactively impose traditional affordability rules onto fundamentally different products.

If the proposed measures around creditworthiness, arrears, and forbearance are intended to apply only to decentralised custodial entities offering cryptoasset lending and borrowing services, then the FCA should explicitly clarify this in its policy proposals. A lack of definitional clarity risks regulatory overreach into decentralised, non-custodial protocols that do not present the same counterparty or operational risks. To ensure proportionality and legal certainty, the FCA should articulate a clear and technologically neutral definition of "custodial lending platforms" and delineate the scope of application accordingly. Without such

clarification, the current framing may unintentionally conflate distinct models and undermine the viability of permissionless innovation in the UK.

For centralised UK-authorised firms, offering custodial lending and borrowing services, applying full CONC requirements is appropriate and should be enforced while for decentralised, non-custodial or technical edge cases, adapted alternatives may better balance innovation and consumer protection.

Question 36: Do you agree that the proposed restrictions for collateral top ups would reduce the risk profile for retail consumers? Are there are any suitable alternatives?

We do not agree that the proposed restrictions on collateral top-ups—namely requiring express consent before the first use of automatic top-ups and imposing limits on the amount that can be automatically topped up—are an appropriate or effective way to reduce risk for retail consumers. While the intention to enhance consumer protection is valid, these measures misunderstand how automated collateral management functions in crypto markets and may unintentionally increase the risk of harm.

In decentralised lending protocols and some centralised platforms, automatic collateral top-ups serve a critical risk mitigation function. They are not a discretionary feature but an essential mechanism that helps borrowers avoid liquidation. The logic is simple: topping up collateral in response to market volatility is far less damaging to the borrower than allowing their position to be liquidated—often at a steep discount and accompanied by penalties. Placing arbitrary limits on these top-ups would strip away one of the few protective mechanisms borrowers currently have and may expose them to unnecessary liquidations during routine market fluctuations.

The proposal to require renewed consent each time the terms of a top-up change also misunderstands the dynamics of rapidly moving markets. Collateral value can fluctuate in seconds. Requiring manual intervention—either in the form of new consents or top-up caps—could force a delay in securing the position, again resulting in liquidations that might otherwise have been avoided. In the fast-paced context of cryptoasset borrowing, time is not a luxury retail borrowers typically have.

Rather than introducing rigid limitations that could undermine automated risk management, a better solution would be to mandate clear, prominent disclosure before loan initiation. Consumers should be made fully aware that auto-top-ups are a core feature of the product, that successive top-ups may be triggered under volatile conditions, and that their position may still be liquidated if margin thresholds are breached despite these protections. Offering borrowers the option to set custom thresholds or opt-in/out of automatic top-ups at the point of agreement would empower them without compromising risk management.

Importantly, DeFi protocols are not equivalent to traditional margin accounts managed by brokers. They rely on self-executing smart contracts with immutable rules. Any attempt to mandate discretionary approvals or impose post-deployment constraints would either exclude permissionless DeFi protocols from compliance or force them to radically centralise—contrary to the innovation they bring.

Question 37: Do you consider the above measures would be proportionate and effective in ensuring that retail consumers would have sufficient knowledge and understanding to access to cryptoasset lending and borrowing products?

We do not consider the proposed measures to be proportionate or sufficient on their own to ensure meaningful consumer understanding, nor do we agree that the complexity of cryptoasset lending and borrowing justifies treating these products as inherently unsuitable for retail consumers. Instead, we believe these products—when properly explained, transparently structured, and appropriately disclosed—can and should remain accessible to retail participants, particularly given their foundational role in decentralised finance.

The core issue is not the intrinsic complexity of lending and borrowing models, but rather the current regulatory gap in how risks are communicated. Much of the harm observed in past market failures stemmed from misleading incentives, unclear terms, or conflicts of interest—not from the products themselves. As such, blanket assumptions about retail capability or a presumption of unsuitability would be counterproductive. What is needed is targeted regulation that raises disclosure standards without restricting access.

If the proposed measures—such as express consent and appropriateness assessments—are intended to apply solely to decentralised custodial entities offering cryptoasset lending and borrowing services, then we consider them appropriate within that limited scope. These firms maintain discretionary control over customer assets and operate with information asymmetries that justify additional layers of consumer protection. However, it is essential that the FCA clearly delineates this scope to avoid misapplying these requirements to non-custodial protocols or decentralised platforms, where such measures would be technologically impractical, legally ambiguous, and counterproductive to the goals of open financial infrastructure.

The proposed measures should be outcome-oriented (focused on actual understanding, not just process), tied to tiered access, where more complex or riskier products are only available to demonstrably knowledgeable consumers. In our view, this approach balances consumer protection with market innovation.

Question 38: What benefits do platform tokens provide to consumers?

Platform tokens, when properly designed and transparently governed, provide a number of benefits to consumers—particularly in cryptoasset lending and borrowing markets. First and foremost, platform tokens create economic alignment between users and service providers. They often serve as a medium for fee discounts, coupons, loyalty rewards, or governance rights, empowering users to influence platform development or risk parameters, which enhance user engagement and decentralised decision-making.

In lending and borrowing contexts, platform tokens can incentivise liquidity provision through yield boosts or reduced collateral requirements, improving overall market efficiency

and deepening liquidity pools. These incentives help bootstrap lending protocols, especially in early-stage ecosystems, by attracting both retail and institutional participation without relying on centralised capital allocation.

Moreover, platform tokens can be used to compensate users for taking on certain risks or helping the system function. For example, some tokens reward users for providing overcollateralised loans or participating in insurance mechanisms. These forms of incentive design are critical for the development of permissionless credit markets, which do not depend on traditional credit scoring or centralised balance sheets.

Question 39: How can conflicts of interest be managed for platform tokens to reduce the risk profile for retail consumers?

Conflicts of interest in platform tokens are real and material, especially for retail participants who may assume they're dealing with neutral market infrastructure. These conflicts can be mitigated with a mix of governance separation, transparency, trading restrictions, and disclosure, all calibrated to the token's risk profile and use case.

The root problem is not the use of platform tokens per se, but the lack of clear disclosures and unchecked centralised control over token supply, liquidity, and pricing mechanisms. These are governance failures—not intrinsic flaws in the utility of platform tokens.

To reduce risks for retail consumers, we propose the following measures. First, platforms should be required to publish a transparent token issuance and burn policy, ideally embedded on-chain and auditable. This would reduce the risk of manipulative practices like undisclosed supply contractions or wallet recycling. Second, there should be mandatory disclosure of the token's role within the platform—whether used for yield boosting, collateral, fee discounts, or governance—along with a plain-language explanation of the associated risks.

Where the platform also operates an internal exchange or facilitates token liquidity, there should be functional separation between the token's treasury management and trading operations. Additionally, any preferential treatment linked to holding or using the platform token—such as enhanced yields—must be clearly disclosed and justified through a published risk/reward rationale.

Finally, where the platform token is used as collateral, it may be reasonable to apply more conservative risk parameters (e.g., lower loan-to-value thresholds or haircuts) than those applied to non-affiliated tokens to reflect potential price volatility and moral hazard.

Question 40: Do you consider that if we are to restrict retail access to cryptoasset lending and borrowing, an exemption for qualifying stablecoins for specific uses within the cryptoasset lending and borrowing models would be proportionate and effective in reducing the level of risk for retail consumers?

No, we do not believe that an exemption limited exclusively to the use of *qualifying stablecoins* in cryptoasset lending and borrowing would be a proportionate or effective

regulatory response. While qualifying stablecoins offer reduced volatility relative to other cryptoassets, their use as a regulatory proxy for "safety" is overly simplistic and risks sidelining the broader benefits and design diversity of decentralised lending and borrowing protocols.

First, volatility is only one dimension of risk. Stablecoins—particularly those pegged to fiat currencies—still carry issuer risk, custodial risk, and depegging risk, all of which have been demonstrated repeatedly in both algorithmic and fiat-backed stablecoin models. Therefore, over-relying on the safety of stablecoins may provide a false sense of security to consumers.

Second, the innovation and resilience of crypto lending and borrowing markets lie in their composability and asset diversity. Restricting retail access to non-stablecoin-based models eliminates consumer choice and penalises the DeFi primitives that underlie real decentralised credit formation—particularly those that allow users to lend or collateralise with highly liquid cryptoassets such as ETH, wrapped BTC, or even tokenised real-world assets. Many of these assets exhibit deep market liquidity and on-chain transparency that, when combined with overcollateralisation and liquidation mechanisms, offer robust risk mitigation in a way that centralised credit products rarely achieve.

Third, the proposed exemption also misunderstands how lending models work in practice. In many DeFi protocols, users choose the collateral and loan asset that best fits their needs and market view. Mandating stablecoins for either input effectively removes one side of the user's agency and undermines the core principle of permissionless finance.

If the concern is excessive risk or consumer harm, a more effective approach would be to assess the adequacy of protocol-level risk controls—such as real-time monitoring of LTV ratios, audit transparency, liquidation penalties, and smart contract security—rather than impose one-size-fits-all restrictions based on asset type. The assumption that stablecoins alone can serve as a universal de-risking mechanism is both flawed and counterproductive.

Chapter 5 – Restrictions on the use of credit to purchase cryptoassets

Question 41: Do you consider that implementing restrictions on the use of credit facilities to purchase cryptoassets would be effective in reducing the risk of harm to consumers, particularly those who could be considered vulnerable? Are there alternative approaches that could equally mitigate the risks?

We do not support a blanket restriction on the use of credit facilities to purchase cryptoassets. While the intention to protect vulnerable consumers from over-indebtedness is important and understandable, a prohibition would be disproportionate, risk distorting the market, and could unintentionally undermine responsible financial inclusion and consumer autonomy. It should be noted that many banks in the UK already block transfer to cryptoasset trading platforms, making it difficult to purchase cryptoassets without using a credit card. Banning credit card use would further disadvantage UK retail users.

First, credit is an essential and ubiquitous financial tool in modern economies. Consumers regularly use credit to purchase a wide range of financial and speculative

products—including equities, foreign exchange, and even high-risk investment schemes. Imposing a unique restriction on cryptoassets based on their volatility while permitting credit-based purchases for other volatile asset classes (such as penny stocks, leveraged ETFs, or derivatives) would create an unjustifiable regulatory asymmetry. This contradicts the principle of technology neutrality and the Treasury's broader commitment to a "same risk, same regulatory outcome" framework.

Second, a complete prohibition would penalise responsible consumers who use credit prudently as part of a broader financial strategy. Not all consumers who purchase cryptoassets with credit are impulsive or financially vulnerable. Many view these assets as part of a diversified portfolio, often repaying their credit balances in full within the billing cycle. A ban would remove a legitimate financial choice from a wide segment of the population without sufficiently distinguishing between those at risk and those who are not.

Third, the proposal overlooks the role of effective disclosures and existing consumer protections under the Consumer Duty and Financial Promotions regime. Rather than prohibiting credit use, it would be more proportionate to mandate firms to assess a customer's risk appetite, provide risk warnings about using borrowed funds to purchase volatile assets, and limit promotional practices that encourage credit-fuelled speculation. This mirrors successful approaches in other sectors where firms are required to disclose risk, rather than eliminate access altogether.

Fourth, restricting credit use could push users toward less transparent or unregulated channels which may expose them to far greater risks, including fraud, exploitative terms, and lack of recourse in case of disputes.

Finally, exempting only *qualifying stablecoins* as a workaround to this restriction is inadequate. Using stability as the sole criterion for credit eligibility could reinforce a false sense of safety among consumers and distort market behaviour in favour of specific asset types or issuers. Additionally, stablecoins are immediately exchangeable into other crypto assets. Furthermore, exempting only *qualifying stablecoins* couldn't work in practice.

Chapter 6 – Staking

Question 42: Do you agree that firms should absorb retail consumers' losses from firms' preventable operational and technological failures? If not, please explain why? Are there any alternative proposals we should consider?

We respectfully disagree with the assumption that firms should automatically and in all circumstances absorb retail consumers' losses arising from staking-related technological or operational failures, even when such failures are deemed "preventable." While we acknowledge the importance of consumer protection, imposing blanket liability on staking providers for all such losses introduces significant unintended consequences that could stifle innovation, restrict market access, and undermine the viability of staking as a foundational layer of Web3 and the decentralised economy.

Staking is a core function of many public blockchain protocols and is essential to maintaining security, decentralisation, and energy-efficient consensus. Penalising staking firms for protocol-level or validator-related risks (especially when not operated directly by the firm itself) imposes a level of liability that is neither proportionate nor feasible given the open and distributed nature of these networks. Slashing, in particular, is a protocol-defined deterrent that aligns validator incentives with network integrity. If a firm is not responsible for validator misconduct, it is inappropriate to hold them accountable for the economic consequences of that misconduct.

We respectfully recommend that non-custodial, native staking on a blockchain should fall outside of the scope of the regulatory regime. Only custodial staking services, where the service provider safeguards the qualified cryptoassets on behalf of another, should be regulated.

Staking-as-a-service, where staking is offered by custodial wallet providers or cryptoasset exchanges acting on behalf of users, should clearly be a regulated activity. These entities exercise control over user assets and present meaningful consumer risk. They operate by way of business and should be subject to authorisation requirements.

Native staking, on the other hand, refers to staking performed directly by users through their own wallets and in direct interaction with the protocol. These arrangements do not involve custody or service provision by a third party. Therefore, they should fall outside the scope of the proposed regulatory framework. The user retains full control, and there is no one acting on their behalf. These activities should not be regulated under this framework.

What the FCA's current framing misses is that staking is not a yield-generating investment product in the traditional sense. Rather, it is a mechanism to participate in and secure the operation of a decentralised network. The act of staking—as practiced on public permissionless blockchains—is fundamentally different from decentralised lending or yield farming. Staking is integrated into the protocol layer itself, and rewards are distributed according to transparent consensus rules. Holding intermediaries liable for outcomes they do not control would force the majority of staking services out of the UK, reducing consumer choice and harming the competitiveness of the UK crypto market.[3][4]

However, if staking is offered as a custodial service—where the provider takes possession of client assets and intermediates the entire staking process—we agree that such firms should be held to a higher operational and technological standard. In those cases, where the provider exercises control over validator selection, slashing mitigation, custody, and reward distribution, liability for preventable failures is a reasonable expectation. In such custodial setups, the firm is actively managing the process on behalf of the user and should be responsible for maintaining the integrity, resilience, and transparency of the service.

[3] SEC's Statement on the threefold classification of staking activities (solo staking, self-custodial staking directly with a third party/validator, custodial staking) (May 29, 2025)
[4] ESMA's binary classification of staking activities under MiCAR (custodial staking and non-custodial staking)

Question 43: Do you agree that we should also rely on the operational resilience framework in regulating staking, including the requirements on accountability?

We agree that the operational resilience framework should apply to custodial staking service providers, provided it is adapted appropriately to the specific context of staking within decentralised networks.

Staking involves a diverse range of operational models—from delegation services provided by decentralised exchanges to fully non-custodial smart contract-based pooling mechanisms. Applying SYSC 15A in a blanket fashion without accounting for this variation risks forcing inappropriate controls on open-source software protocols or pushing staking services toward centralisation to meet compliance requirements.

Instead, operational resilience for custodial staking providers should focus on safeguarding customer assets, maintaining accurate records, monitoring validator performance, and mitigating known counterparty risks. Where a firm actively selects or operates validators, there should be clear standards for due diligence, validator uptime monitoring, and transparency on commission structures. However, this framework should remain *proportional* and avoid treating open participation in consensus protocols as equivalent to offering financial products or investment services.

We also recommend that the FCA recognise that overregulation of staking intermediaries could unintentionally push consumers toward less transparent or riskier staking alternatives, including offshore platforms and pseudo-anonymous smart contracts beyond the FCA's reach. A flexible, principles-based application of the operational resilience regime—tailored to the risk profile and technical role of the firm—is the best way to ensure that consumers are protected without impairing the development of staking as a key enabler of Web3 infrastructure.

Question 44: Do you agree that firms should have to get express consent from retail consumers, covering both the value of consumer's cryptoassets to be staked and the type of cryptoassets the firm will stake, with each cryptoasset staked by the consumer requiring its own consent?

Yes, we agree that custodial staking providers should be required to obtain express, asset-specific consent from retail consumers prior to staking their cryptoassets. This requirement is essential for maintaining transparency, preserving consumer autonomy, and upholding trust in the staking process. Since custodial staking involves the transfer of control and operational use of a customer's assets — which may include delegation or locking mechanisms and potential slashing risks — it is crucial that consumers are fully informed about what assets are being used, how, and under what terms. Additionally, firms should clearly communicate the purpose of staking, associated risks (such as slashing, unbonding delays, or potential loss of rewards), and any relevant protocol-level mechanics, in plain language.

Question 45: Do you agree that firms should provide a key features document as outlined above to retail consumers? If not, please explain why? What other means

should be used to communicate the key features and risks of staking to consumers?

We agree that a key features document could be an effective tool to improve transparency and consumer understanding—if implemented proportionally and tailored to the nature of staking, not copied wholesale from investment product disclosures. However, it is important to clarify that this requirement should apply specifically to custodial staking providers. These entities act as intermediaries and hold discretionary control over client funds, which introduces a layer of risk and responsibility that justifies clearer disclosures. For non-custodial, user-directed staking through self-custodied wallets, such measures would be inappropriate and infeasible.

We recommend that the FCA clearly distinguish staking from yield-bearing financial instruments like lending or speculative "earn" programs. Unlike cryptoasset lending, staking operates under open consensus protocols with transparent on-chain logic and verifiable incentives. The proposed key features document must reflect this distinction and not unintentionally mislead consumers into believing that staking is akin to traditional financial products.

The document should be concise and technical without being legalistic. A suggested best practice could be a two-tiered approach:
– A summary sheet outlining core features (e.g., lock-up period, reward mechanism, fees, slashing risk, third-party validator info);
– A deeper technical explainer, optionally available for users wanting further detail.

In our opinion, a Key Features Document should be mandatory for custodial staking providers. It's a practical, proven, and proportionate way to: i) improve consumer understanding; ii) prevent mis-selling and disputes; iii) and strengthen regulatory compliance and accountability. The KFD should be complemented by layered digital disclosures, point-of-decision prompts, and clear post-sale reporting to ensure consumers understand and remain informed throughout the staking process.

Question 46: Are there any alternative proposals we should consider to minimise the risks of retail consumers' lack of understanding leading to them making uninformed decisions?

The FCA's framing throughout this Discussion Paper reveals a recurring and problematic assumption: that retail participants in cryptoasset markets are fundamentally incapable of making informed decisions, and therefore require broad-based protection from themselves. This paternalistic view conflates consumer protection with consumer restriction, and it risks alienating the very group of individuals who are actively exploring, experimenting with, and adopting decentralised technologies by choice—not ignorance.

It is a mistake to treat all retail participants as inexperienced or vulnerable investors simply because they choose to engage with staking, DeFi, or other protocol-level activities. Many of these individuals are not passive consumers of speculative financial products but rather active participants in open infrastructure, drawn to crypto precisely because of its permissionless and transparent nature. To categorise them as victims in need of shielding by

default is not only reductive but also dismissive of the significant technological literacy and financial agency that many users possess in these markets.

This stance also reflects a fundamental misunderstanding of the ethos and architecture of decentralised finance. DeFi is not designed to outsource responsibility to decentralised gatekeepers or intermediaries. Instead, it invites users to take control of their financial interactions, with all the risks and freedoms that entails. While there is certainly a need for safeguards against fraud or malicious conduct, this does not justify erecting barriers to entry under the guise of protection—particularly in areas like staking, where the economic incentives are protocol-governed, and risks can be transparently communicated.

By painting retail users as inherently naïve, the FCA risks overcorrecting and enacting measures that not only fail to improve outcomes but also remove agency, limit innovation, and force users to seek alternatives in unregulated or offshore environments. This creates a false sense of safety while pushing meaningful activity—and the opportunities for user-driven financial empowerment—out of the UK.

True consumer protection in the crypto space should begin with respecting the intelligence and intent of retail users. It should focus on equipping them with better information, more transparent tools, and clear rights—not arbitrarily denying access to participation in foundational systems like staking and DeFi.

Question 47: Do you agree that regulated staking firms should be required to segregate staked client cryptoassets from other clients' cryptoassets? If not, why not? What would be the viable means to segregate clients' assets operationally?

We agree that regulated custodial staking firms should be required to segregate staked client cryptoassets from other clients' cryptoassets. Segregation of assets is a foundational principle in safeguarding arrangements and is particularly important in the context of staking, where the operational use of assets by the service provider (e.g., delegation, bonding, locking) introduces additional risks beyond standard custody. Segregating staked assets by client — or at least by staking product — can significantly reduce the impact of loss events, mitigate conflicts of interest, and enhance auditability and client confidence in the firm's practices.

Operational segregation can be achieved through the use of distinct wallet structures, leveraging either individual wallets per client or product-level wallets with robust internal records and reconciliation systems. In cases where blockchain-level wallet fragmentation is not feasible due to cost or protocol limitations, firms should implement strong off-chain segregation through detailed ledgering, wallet labelling, and frequent reconciliations. These mechanisms can ensure client positions are always transparently attributable and protected from the firm's own obligations or liabilities. Segregation also reinforces the principle that staked assets remain under the beneficial ownership of clients and not the firm, which is essential for legal clarity in case of insolvency or disputes.

Question 48: Do you agree that regulated staking firms should be required to maintain accurate records of staked cryptoassets? If not, please explain why?

We agree that maintaining accurate records of staked cryptoassets is essential, but we recommend that the FCA limit this requirement strictly to custodial staking firms. It is vital to recognise that not all firms engaged in staking custody user assets, and not all blockchains or staking models operate through custodial intermediaries. Blanket application of record-keeping obligations to non-custodial or protocol-native staking arrangements would be both inappropriate and counterproductive.

Staking is, in many cases, a protocol-level function governed by transparent, immutable, and auditable rules embedded in the consensus layer of public blockchains. In such designs users may stake directly from their own wallets or interact with smart contracts that automatically allocate, track, and return staked balances without any third-party custody. In these instances, the ledger itself already functions as the record-keeping system, with superior reliability, resilience, and transparency compared to any off-chain firm-maintained ledger.

Imposing record-keeping obligations on firms that do not hold custody or have no control over the staked assets would introduce redundant processes and increase operational costs without delivering any meaningful consumer protection benefit. This could also disincentivise the development of non-custodial staking infrastructure, undermining the FCA's own goals of promoting innovation and market integrity.

We therefore recommend that the FCA clearly delineate between custodial and non-custodial staking in its regulatory approach. Record-keeping should be required only for entities that act as custodians and stake cryptoassets on behalf of retail consumers. These entities must be able to demonstrate, with precision and on demand, which assets have been staked, on behalf of whom, and with what expected outcomes in terms of rewards or penalties.

This approach strikes the right balance between protecting consumers in cases of firm failure or operational misconduct while preserving the viability of decentralised and user-controlled staking architectures that do not introduce intermediary risk in the first place. Regulatory clarity on this distinction is critical to avoid conflating fundamentally different staking models and to ensure that rules are applied in a proportionate and technically appropriate manner.

Question 49: Do you agree that regulated staking firms should conduct regular reconciliations of staked cryptoassets? If not, please explain why? If so, what would be the appropriate frequency?

We agree that regulated custodial staking firms should be required to conduct regular reconciliations of staked cryptoassets. However, this requirement should not be imposed indiscriminately across all staking models. It should apply only to firms that assume custody and operational control over client assets during the staking process. Regular reconciliation is a critical control to ensure that client assets are properly accounted for, secure, and aligned with both on-chain data and internal records.

In the case of non-custodial or protocol-native staking, where consumers retain control over their private keys and interact directly with smart contracts or the consensus layer, the

concept of reconciliation becomes redundant. The public ledger itself functions as the definitive and immutable source of truth. For these systems, on-chain data provides full transparency, auditability, and real-time accuracy, far exceeding the assurances offered by any firm-maintained records.

For custodial staking firms, reconciliation is necessary to ensure the integrity of operations and prevent shortfalls, misallocations, or incorrect reward distributions. In such cases, reconciliations should cover not just balances, but also validator allocations, pending reward accruals, and any penalties such as slashing that may have occurred. These checks are important to maintain consumer trust and operational accountability.

As for the appropriate frequency, this should be risk-based and proportionate to the size and complexity of the firm's staking operations. A daily reconciliation may be excessive for low-volume custodians or firms supporting blockchains with infrequent validator cycles, while it may be entirely appropriate for larger custodians handling significant volumes or staking on high-frequency protocols. The FCA should avoid prescribing a one-size-fits-all frequency and instead allow for a tiered approach based on firm size, staking volume, and technological infrastructure.

Finally, as stated in our previous responses, it is critical that the FCA clearly limits this requirement to custodial entities. Imposing reconciliation obligations on non-custodial protocols or self-custody models would not only be impractical, but would also conflate fundamentally distinct architectures, undermining both regulatory clarity and innovation in the UK crypto ecosystem. A regular reconciliation of staked cryptoassets is essential for accuracy, client protection, regulatory compliance, and trust. Ideally, firms should reconcile daily, but at minimum monthly reconciliation should be mandated, with frequency adjusted for firm size and risk profile.

Chapter 7 – DeFi

Question 50: Do you consider the proposed approaches are right, including the use of guidance to support understanding? What are the effective or emerging industry practices which support DeFi participants complying with the proposed requirements in this DP? What specific measures have you implemented to mitigate the risks posed by DeFi services to retail consumers?

We respectfully submit that the current proposed approach, while well-intentioned, risks mischaracterizing the unique properties and systemic value of DeFi. We advocate for a proportionate, technologically informed, and innovation-positive framework—one that distinguishes decentralised systems from superficially decentralised business models. DeFi, when implemented properly, is not a replication of decentralised finance on a blockchain, but a fundamental redesign of financial architecture with embedded transparency, programmability, and self-custody.

We support the use of *guidance*—not rules—as the primary regulatory tool for interacting with the DeFi ecosystem. The dynamic and composable nature of DeFi means that rigid compliance frameworks quickly become obsolete or counterproductive. Instead, iterative guidance developed in close collaboration with developers, researchers, and decentralised governance communities will yield more sustainable and innovation-aligned outcomes. Guidance also allows for a differentiated regulatory approach that reflects varying levels of decentralisation, without forcing diverse architectures into a legacy compliance model.

Critically, we recommend that the FCA preserve and respect the Treasury's clear signal in the draft RAO SI that truly decentralised protocols should remain outside the scope of direct regulation. This is not a loophole—it is a principled recognition that when there is no identifiable controlling party, the risk dynamics are fundamentally different. The resilience of public infrastructure, open-source smart contracts, and autonomous validation mechanisms should be seen as a strength of DeFi, not a regulatory gap.

Where protocols do involve identifiable intermediaries or semi-decentralised components, we support a *graduated and proportionate* approach. Emerging practices such as third-party security audits, open governance frameworks, real-time on-chain analytics, and formal verification of smart contracts already offer industry-led mechanisms to mitigate operational risk and enhance consumer protection without undermining decentralisation. These mechanisms should be actively supported—not replaced—by regulators.

The proposals outlined in provisions 7.4 through 7.10 suggest a profound misunderstanding of the structural and operational differences between decentralised and decentralised systems. While we acknowledge the Treasury’s stated intention to exclude "truly decentralised" protocols from regulatory scope, the framework being built around this intention appears both ambiguous and overreaching. Paragraph 7.4 opens the door to discretionary enforcement by failing to provide a clear, technical definition of what constitutes "a clear controlling person." In the DeFi ecosystem, control is often distributed among token holders, multisig councils, or DAO structures—not a single legal entity or operator. Without specificity, this vague language creates legal uncertainty and invites inconsistent regulatory application.

Moreover, paragraph 7.5 conflates technological neutrality with regulatory symmetry. The assertion that "activities posing the same risks should have the same regulatory outcomes" ignores the fact that decentralisation fundamentally changes the nature, source, and mitigation of risks. In decentralised systems, enforcement is coded, permissions are automated, and custody is typically user-controlled. To impose the same compliance architecture as that designed for decentralised custodians is not a form of equal treatment—it is a denial of the architectural advantages of decentralisation. The result would be the regulatory flattening of two distinctly different paradigms, and the forced migration of innovation away from the UK market.

Paragraph 7.6 asserts the need for a “consistent framework” for all entities conducting regulated activities. However, consistency must not come at the expense of proportionality. DeFi systems are public goods—many are developed by global communities, operate permissionless, and cannot be retrofitted to match frameworks built for private companies.

Requiring the same rulebook for Uniswap as for Coinbase is not just a category error—it's a policy choice that undermines the design principles of open-source finance. Uniform enforcement may sound fair in theory, but in practice, it suppresses one model (decentralised public infrastructure) in favour of another (decentralised regulated intermediaries). This would be a form of de facto exclusion masquerading as parity.

The reference in 7.7 to operational resilience concerns from smart contracts also reflects a flawed comparison. Smart contracts are not inherently more fragile than decentralised infrastructure—in fact, their transparency and determinism often make them more auditable and secure. Most critical DeFi protocols undergo rigorous formal verification, third-party audits, and public code reviews. The resilience risks that materialised in past crypto failures (as outlined in Chapters 2-6) were largely due to discretionary management, opaque leverage, and custodial mismanagement—not immutable, open-source logic. Treating automation as a liability rather than a safeguard overlooks the very real systemic advantages that DeFi brings to financial markets.

Finally, the proposed application of all rules in Chapters 2-6 to DeFi under paragraph 7.10 is problematic. These chapters were written with decentralised custodians, credit providers, and principal-based trading venues in mind. Extending these same frameworks to DeFi would lead to overregulation by misalignment—forcing DAOs and smart contracts to comply with structures they cannot meaningfully interact with (e.g., affordability assessments, client asset segregation, or explicit consent protocols). If the FCA truly wants to avoid regulatory arbitrage, it should first ensure that its perimeter is technologically literate. Otherwise, the UK's approach will simply drive decentralised innovation offshore while protecting only those incumbents capable of absorbing compliance costs.

In summary, we recommend that the FCA adopt an agile, proportionate and collaborative stance on DeFi. Regulation should reinforce the core principles of decentralisation—not dilute them. The goal must not be to retrofit DeFi into the mold of TradFi, but to ensure that public, decentralised financial systems remain transparent, safe, and open to all.

Conclusion

Question 51: We consider these potential additional costs to firms and consumers in the context of the potential benefits of our proposed approach, set out earlier in Chapter 1. In your view, what are the costs of these different approaches? Can you provide both quantitative and qualitative input on this.

We believe the costs of the proposed regulatory approach—particularly where rules designed for traditional financial services are applied wholesale to cryptoasset firms and decentralised systems—are likely to be disproportionately high in both financial and innovation terms. Without clearly defined proportionality, technological nuance, and scope limitation, the cumulative burden risks stifling competition, forcing smaller firms out of the UK market, and discouraging the development of open, permissionless infrastructure.

Qualitative costs stem primarily from compliance misalignment. Many of the proposed rules—such as creditworthiness assessments for overcollateralised crypto lending, segregation of client assets in technically indivisible staking contracts, or mandatory disclosures modeled after regulated securities products—do not align with the operational design of crypto protocols. For firms, this mismatch introduces compliance uncertainty, legal risk, and operational complexity. For consumers, the cost is indirect but substantial: reduced product access, less innovation, and the increased likelihood of being pushed into unregulated offshore markets with fewer consumer protections.

Moreover, if all firms—regardless of size, business model, or level of centralisation—are subjected to the same regulatory treatment, this will entrench large custodial incumbents and penalise newer, leaner, or decentralised players. Regulatory regimes that fail to scale with risk and business size will inevitably result in market consolidation, less competition, and fewer consumer choices. Many firms may opt out of the UK entirely, reducing the jurisdiction's long-term competitiveness in the global crypto economy.

Quantitatively, the cost impact varies significantly depending on the scope of the rules. Internal estimates from UK-based crypto intermediaries suggest that aligning operations with proposed frameworks (including client classification, disclosure templates, real-time trade reporting, and staking segregation) could significantly increase operational and legal expenses for small-to-mid-sized firms. For firms operating or integrating DeFi infrastructure, costs would be even higher due to the need to introduce decentralised compliance layers that may be fundamentally incompatible with their architectures—costs that are difficult to estimate precisely but would likely exceed six to seven figures in initial development, with ongoing legal and regulatory liabilities.

Question 52: Do you agree with our assessment of the type of costs (both direct and indirect) and benefits from our proposals? Are there other types of costs and benefits we should consider?

We acknowledge the FCA's effort to map both direct and indirect costs and benefits of the proposed regime. However, we believe the current assessment underestimates the true scope of indirect costs, particularly those related to innovation displacement, regulatory uncertainty, and the erosion of competitiveness for UK-based crypto and Web3 firms. While consumer protection is a valid objective, this must be balanced carefully against the long-term structural benefits of fostering open, programmable, and permissionless financial systems.

The most significant omitted cost is regulatory misfit—that is, the operational and compliance burden created when frameworks developed for traditional finance are applied to crypto-native business models without sufficient technological understanding or contextual nuance. For example, applying creditworthiness assessments to overcollateralised, non-custodial lending, creates friction that serves no meaningful risk-reduction purpose but imposes costly compliance requirements. These requirements are particularly damaging for small and mid-sized firms and may lead to market consolidation around large

custodians—the opposite of the competition and consumer choice objectives laid out in Chapter 1.

We recommend that the FCA more clearly distinguish between consumer-facing risks driven by centralised misconduct and the structural characteristics of decentralised permissionless systems. Many of the harms cited in the consultation—such as asset rehypothecation, hidden leverage, and mispriced yield—are a consequence of opaque decentralised business models, not of crypto markets as a whole. If regulation imposes identical requirements on both decentralised and custodial models, it risks removing the very mechanisms (e.g., smart contract automation, open-source transparency, and self-custody) that mitigate these risks by design.

Another overlooked indirect cost is jurisdictional arbitrage. If the UK adopts a rigid or ill-fitting regulatory regime, firms may simply migrate activity to more innovation-friendly jurisdictions. This leads not only to economic loss but also to reduced consumer protection for UK residents who may continue to access offshore platforms without oversight. Conversely, a clear, innovation-compatible regulatory environment can attract responsible firms and foster domestic industry growth—an opportunity cost that should be incorporated into the cost-benefit analysis.

Question 53: How do you see our proposed approach to regulating these activities affecting competition in the UK cryptoasset market?

If adopted without refinement, these proposals would reduce competition in the UK cryptoasset market by tilting the playing field in favor of large, heavily capitalised, custodial institutions and decentralised exchanges. Smaller firms and DeFi projects would face operational and legal thresholds that many cannot realistically meet.

The effect would be a consolidation of market power into a handful of UK-licensed entities, leading to reduced consumer choice, slower product innovation, and weakened alignment with open-source communities that prioritise privacy, decentralisation, and transparency. For UK consumers, this could mean fewer safe, decentralised alternatives, and more exposure to decentralised service failures—the very risks these regulations aim to address.

Question 54: Are there any additional opportunities, including for growth, we could realise through a different approach to regulating these activities?

Yes, there are several missed opportunities for growth that could be realised through a more innovation-aligned, differentiated approach to regulating cryptoasset activities. The UK has a unique chance to establish itself as a global hub for responsible digital asset innovation—but to do so, it must move beyond retrofitting legacy regulatory models onto novel technologies and instead adopt a bespoke framework that recognises the diversity of crypto business models, including those that are open-source, decentralised, and non-custodial.

A more nuanced treatment of decentralised systems is a key area of opportunity. The UK could lead by providing regulatory clarity that distinguishes between protocol-level

infrastructure with no identifiable controlling party and centralised service providers that custody user funds. Rather than applying identical compliance burdens to both, the UK could develop a tiered framework that encourages innovation in open financial infrastructure while holding custodial entities to higher standards of consumer protection. This would signal to developers and builders that the UK understands and respects the principles of permissionless innovation, attracting top global talent and capital. We also recommend the introduction of a tailored innovation sandbox with pre-approved compliance plug-ins (e.g., KYC, trade monitoring) via open APIs—allowing startups to experiment safely and scale faster within a clear, low-friction regulatory environment.

A more flexible, innovation-friendly regulatory approach—balanced with consumer protection—can: i) encourage product and business model innovation; ii) lower barriers for startups; iii) foster market competition; iv) build consumer trust through self-regulation and technology; and v) ultimately drive market growth and global competitiveness.

While regulation is necessary, we must avoid applying a one-size-fits-all framework that would overburden the very systems that offer greater transparency, automation, and disintermediation. A forward-looking regime—one that protects consumers without undermining decentralisation—is the only path to sustainable leadership in the Web3 era.