ICAEW
REPRESENTATION 43/25

DP25/1: REGULATING CRYPTOASSET ACTIVITIES

Issued 13 June 2025

ICAEW welcomes the opportunity to comment on the DP25/1: Regulating cryptoasset activities published by the Financial Conduct Authority (FCA) in May 2025, a copy of which is available from this link.

This response of 13 June 2025 has been prepared by the ICAEW Financial Services Faculty. As a leading centre for thought leadership on financial services, the faculty brings together different interests and is responsible for representations on behalf of ICAEW on governance, regulation, risk, auditing, and reporting issues facing the financial services sector. The faculty draws on the expertise of its members and more than 25,000 ICAEW members involved in financial services.

The ICAEW Digital Assets Working Party (DAWP) was formed in February 2023 to share knowledge and influence policy around digital assets. It is a multi-disciplinary working party with experts across accounting, law, academia, regulation, and technology. It has workstreams focused on audit and assurance, financial reporting, the future of digital assets, regulation, and tax. This publication has been developed by the DAWP Steering Committee which is coordinated by the ICAEW Financial Services Faculty and whose members include experts from professional services firms, industry, and other bodies. This publication does not represent the views of individuals or firms.

ICAEW is a world-leading professional body established under a Royal Charter to serve the public interest. In pursuit of its vision of a world of strong economies, ICAEW works with governments, regulators and businesses and it leads, connects, supports and regulates more than 172,000 chartered accountant members in over 150 countries. ICAEW members work in all types of private and public organisations, including public practice firms, and are trained to provide clarity and rigour and apply the highest professional, technical, and ethical standards.

ICAEW
Chartered Accountants' Hall Moorgate Place London EC2R 6EA UK
icaew.com

The Institute of Chartered Accountants in England and Wales (ICAEW) incorporated by Royal Charter (RC000246)
Registered office: Chartered Accountants' Hall Moorgate Place London EC2R 6EA UK

KEY CONCLUSIONS

1. Overall, we support the government's ambition for the UK to be home for the most open, well-regulated, and technologically advanced capital markets in the world. We see the Financial Conduct Authority (FCA)'s vision as set out in the discussion paper as a good first step in the process for the UK to establish a proportionate, clear regulatory framework which enables firms to innovate at pace, while maintaining financial stability and clear regulatory standards.
2. We however would emphasise caution at this point in the regulatory journey. Where the technology is still immature and the private sector is likely to see both wins and fails in respect of use cases and investment propositions, there will always be heightened risks. These risks can become consequential, be that from a conduct, investor loss or market stability perspective, as the asset class and underlying technology are developing within financial services. For this reason, the design of the regulatory regime should set a high bar; not such that it is overly prohibitive to innovation and investment, but that it sets clear guardrails and expectations for actors in the sector.
3. To strike the right balance, we believe that a mixture of prescription and principles are needed at this time. Clear and prescriptive rules are welcome where the risks of harm are known and are more likely absent regulation. Here, we see the adoption of rules borne out of lessons learned from traditional finance as a pragmatic foundation, enhanced for recent failings in the crypto sector such as FTX, Celsius and others. Principles on the other hand will be needed where our understanding of business models, use cases and associated risks and opportunities are less well understood. This is where, for example, the Consumer Duty might act as a critical backstop to the regime. We encourage the FCA to remain vigilant to market developments and willing to reassess whether rules are fit for purpose as the sector matures.
4. We believe that the rules and expectations around regulated cryptoasset activities should draw a clear distinction between products and services offered to retail as opposed to institutional customers.
5. While not directly referred to in the discussion paper we believe that more needs to be done between regulators to ensure the UK has a coherent approach to cryptoassets.
6. Legal, tax, financial reporting and assurance form the backbone of building consumer trust in the nascent area of cryptoassets. In our view, it is necessary that an approach considers financial services regulation alongside the ambiguities that exist from a legal, tax, financial reporting, and assurance perspective. A siloed approach may lead to divergence in practices and treatments, which may in turn stifle innovation and investment.
7. While we note that this is not exclusively a matter for the FCA we believe you have a vital role in understanding the challenges that exist across these areas and their potential impact on regulated firms and customers.
8. We recommend greater cross-engagement between the FCA, Law Society, Financial Reporting Council, and professional bodies to further understanding and ultimately to provide greater clarity. The ICAEW along with members and practitioners in the sector are exploring these challenges and would be happy to engage with the FCA along with other regulators if this would help further understanding.

EXECUTIVE SUMMARY

9. We support the principle that **"same risk, same regulatory outcome"** should apply to cryptoasset activities, regardless of the technology used. This is consistent with international standards and avoids regulatory arbitrage.
10. Our responses to the discussion paper reflect an **extension of the best practices, from existing traditional finance (Trad-Fi) where possible** (e.g. application of Client Assets Sourcebook (CASS) rules to the custody of cryptoassets), amended where required to reflect the idiosyncrasies of cryptoassets.
11. **Retail customer losses in the context of staking:** We support the principle that firms should be accountable for retail customer losses resulting from preventable technical and operational failures, aligning with standards like the EU's Digital Operational Resilience Act (DORA). However, greater clarity is needed on the scope of this requirement—specifically, what constitutes a "preventable" event, and which third-party or blockchain-related incidents fall outside a firm's control.
12. Clear guidance will ensure legal certainty for firms and realistic expectations for consumers, who may otherwise assume compensation covers all losses, including those from market movements. Any such framework should balance consumer protection with the operational and capital burdens placed on firms, which could limit market participation and innovation. Alternatives such as slashing insurance, risk-tiered product options, capital buffers, or tailored compensation schemes can be explored to ensure proportionality and sustainability in the regime.
13. We note that the DP only covers retail customer losses in the context of staking at this point and recommend the regulator consider whether the perimeter may need to extend to other cryptoasset activities.
14. **Operational resilience for staking:** We consider the FCA's operational resilience framework to be a sound regulatory base for staking. It is broadly aligned with DORA in its principles, but could benefit from specific enhancements to third-party oversight, incident reporting, and contractual controls.
15. Leveraging DORA as a benchmark can help ensure greater clarity, cross-border consistency, and consumer confidence.
16. The FCA should also consider the operational resilience of critical third parties involved in staking and assess whether to extend the Critical Third Parties Sourcebook to staking firms, especially where firms may become systemic.
17. **Decentralised Finance (DeFi):** We support the FCA's guidance-led, activity-based approach to DeFi and we recommend building regulatory capacity around three pillars:
    - Perimeter clarity through use-case examples and Decentralised Autonomous Organisation (DAO) governance thresholds;
    - Proportional compliance tools (e.g. front-end standards, safe harbour disclosures); and
    - Industry engagement via sandbox initiatives or technical consultation panels.
18. This measured approach can ensure retail users receive appropriate protection without undermining DeFi innovation or its benefits for financial inclusion, resilience, and transparency.
19. **Scoped exemption for qualifying stablecoins:** We agree a carefully scoped exemption, for qualifying stablecoins used as loan or collateral assets can reduce consumer risk, preserve access to lower-risk financial innovation, and avoid the bluntness of an outright prohibition and the unintended consequence of pushing activity offshore. This approach aligns with the FCA's stated goals of proportionality, consumer protection, and sustainable market growth.
20. To ensure consumer protection and market integrity, the exemption should be tightly defined—limited to transactions involving qualifying stablecoins, excluding platform tokens, and subject to caps and Consumer Credit sourcebook (CONC)-style protections. Clear regulatory guidance is also essential on how retail customers would be protected if an issuer collapses, the stablecoin loses value, or fiat reserves are insufficient to support redemptions.

21. **Segregation of staked cryptoassets and maintenance of records:** We support the FCA's proposal that regulated staking firms be required to segregate staked client cryptoassets and maintain accurate records. Segregation enhances client protection and can be implemented through various models, including individual wallets, omnibus wallets with internal tracking, or smart contracts programmed to manage allocations. Firms should clearly communicate segregation practices, in client agreements, to ensure legal clarity and transparency. Accurate recordkeeping is also essential, mirroring CASS standards, and should reflect real-time changes in staking positions and rewards. Firms must also consider any intermediaries in the staking chain and obtain informed, express consent from retail clients, regarding the terms, risks, and fees associated with staking.
22. Furthermore, in our view, an absence of regulation around wallet-providers in the DP could give rise to an issue given that all of these regulated activities will need an end point right where crypto is directed.
23. **Frequency of the reconciliation of staked cryptoassets:** We support the FCA's proposal for regular reconciliation of staked cryptoassets by regulated staking firms, as it is essential for client asset protection, operational integrity, and regulatory compliance. Accurate reconciliations ensure that client holdings reflect rewards and slashing penalties correctly, reduce the risk of errors or shortfalls, and align with existing standards under CASS. Given the 24/7 nature of crypto markets and the complexity of some staking models, a more frequent reconciliation schedule — daily for high-volume firms and weekly as a minimum for others — would be appropriate, with flexibility based on factors such as transaction volume, third-party validators, and blockchain-specific rules.
24. While blockchain technology provides transparency and real-time data to support reconciliation, challenges remain due to pooled custody, off-chain abstractions (e.g. IOUs), inconsistent validator structures, and lack of client metadata on-chain. Complex platforms — such as those offering liquid staking or using synthetic tokens — require bespoke reconciliation tools and processes. The FCA should ensure a proportionate approach that reflects these operational realities, while maintaining robust client protection.

ANSWERS TO SPECIFIC QUESTIONS

CHAPTER 2 – CRYPTOASSET TRADING PLATFORMS

Q11. 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?

25. There are significant potential risks associated with allowing a CATP to admit assets on their platform in which they have a direct or indirect material interest, including:
    1. **Financial crime/Rug Pulls** – where the issuer can manipulate the market around the asset on their own platform, significantly increasing or decreasing the value, in line with their own/associated parties' interests and at the detriment to the wider public/user base.
    2. **Insider trading** – where those associated with the CATP will have prior knowledge of internal events which may influence the price of the issued asset, creating an unfair advantage in relation to trading.
    3. **Tax obligations** – the CATP could purposefully influence the value of the tradeable asset in order to provide themselves with a more beneficial Tax picture.
26. A clear legal, and transparent, separation will be needed to ensure these risks are mitigated appropriately.

Q15. 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?

27. Yes, we agree that CATPs should be subject to both pre-trade and post-trade transparency requirements. The requirements set out in the FCA Handbook pertaining to financial

instruments can be adapted to the markets in cryptoassets. CATPs should make information available to the public on a continuous basis, during normal trading hours. The information provided should include: the range of current bid and offer prices, and the depth of trading interests at those prices. This information should be displayed through their systems for cryptoassets. This requirement should also apply to actionable indication of interests.

28. As proposed, any market participant should be permitted to use and compare information from different execution venues. Both pre-trade and post-trade transparency data should be made available to the public in an 'unbundled' fashion, to reduce costs for market participants when purchasing data. This way would allow public monitoring, for the public interest, of potential systemic risk or fraudulent activities that may transpire.
29. Noted that the DP is not proposing waivers for pre-trade transparency requirements, as it is likely to be too early to define specific liquidity thresholds for different assets.
30. Permitting waivers or deferred publication for some players, may allow for arbitrage and result in inconsistency and unreliability of cryptoasset data across markets. Therefore, to ensure efficient pricing that promotes fair markets and a level playing field for all firms or venues providing trading services, waivers or exemptions from pre-trade transparency or adaptations of the requirements in relation to deferred publication should be available only in certain defined cases. Article 9 of Regulation (EU) No 600/2014 on Markets in Financial Instruments (MiCA) can be set as an initial benchmark, as not much guidance can be obtained from MiCA on this aspect.

Q16. Which challenges may emerge for transaction data requirements if there is direct retail participation?

31. The effectiveness of markets must be considered to ensure that retail investors can make appropriate decisions. Whilst we agree that the FCA must ensure that consumer protections are in place, enabling retail investors to make reasoned and considered transactions must be a primary objective.
32. We note that the FCA recognises that retained transactions may be recorded to include personal tax information such as a National Insurance Number (NINO). It must be noted that as of 1 January 2026, CATPs will generally have reporting obligations under the Cryptoasset Reporting Framework (CARF) being introduced by HMRC.
33. CARF introduces to the UK an ongoing commitment to provide information on an annual basis. This will require CATPs to record information in a way that enables reporting to HMRC. More information on CARF can be found at https://www.gov.uk/government/collections/reporting-to-hmrc-if-you-provide-cryptoasset-services-in-the-uk
34. Currently, the lack of a reporting standard means that CATPs do not record uniformly, which can result in data quality that is often patchy and can be quite poor for some CATPs.
35. Software is available to assist retail customers in calculating their tax obligations. The absence of data reporting standards increases the difficulty for tax calculator software to analyse information.
36. The software is also helpful for retail investors in keeping track of their portfolios more generally. Enabling greater portfolio management across different CATPs would allow retail investors to make considered decisions about their investment activity.
37. We recommend a method that enables CATPs to meet their obligations under CARF, which would significantly reduce the burden on software providers from a UK perspective.

Q17. Are there preferred standards for recording transaction data?

38. See question 16.

Q18. What opportunities and challenges do you see in trying to harmonise on-chain and off-chain transactions' recording and/or reporting?

39. Harmonising the recording and reporting of on-chain and off-chain transactions presents a strong opportunity to improve market transparency, regulatory oversight, and operational efficiency but comes with a number of practical challenges.
40. A unified framework would give regulators a clearer, more comprehensive view of market activity, helping to detect misconduct and systemic risk more effectively. It would also support the creation of a more complete and reliable dataset, enabling better analytics, market insights, and policy development.
41. For market participants, especially investors, this could lead to greater trust, clearer audit trails, and potentially more accurate positions in the event of a firm's insolvency. Over time, greater automation and streamlined reporting could reduce duplication, lower costs, and increase the efficiency of compliance processes.
42. However, this comes with significant challenges: integrating fundamentally different systems—such as the transparent, immutable nature of public blockchains with the privacy requirements of traditional financial systems—is technically and legally complex.
43. On-chain data tends to be immutable and publicly visible, whereas off-chain systems often rely on private data subject to strict confidentiality and data protection rules. Harmonising the two raises legal and operational challenges around privacy and compliance.
44. Implementation costs could be substantial, particularly for smaller firms that may lack the resources to overhaul or adapt existing systems.
45. Additionally, there may be resistance from some parts of the market about merging transaction reporting obligations and putting pressure on existing companies to change / update their reporting processes.
46. The fast pace of technological change also introduces the risk that any harmonised solution could become outdated quickly, requiring continual updates and investment.

CHAPTER 3 – CRYPTOASSET INTERMEDIARIES

Q20. 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)?

47. The main issue we see with requiring firms to check the pricing for an order across at least three K-authorised trading platforms (where available) is it is unclear what firms should do in the lead up and there are no UK-authorised trading platforms – we welcome clarity on this.

Q24. 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?

48. Allowing retail customers to direct execution may undermine best execution obligations. Risks include:
    - Customers may lack the expertise to select appropriate execution venues, increasing the risk of suboptimal outcomes such as poorer pricing, reduced liquidity, and higher costs.
    - Less reputable or lightly regulated venues may also present greater operational and cybersecurity risks.
    - Additionally, fragmentation of orders can impair execution quality by diluting liquidity.
49. Firms remain accountable for execution quality, and regulatory exposure remains even where client instructions are followed.
50. Firms can mitigate the above risks as follows:

- Client agreements should include risk warnings and require explicit consent acknowledging potential deviations from best execution.
- Firms should define when such overrides are permitted and ensure governance frameworks support compliance.
- Regular reviews, audits, and monitoring by Compliance and Risk functions are essential.
- Maintain detailed documentation and audit trails to evidence compliance.
- Limit customer-specified execution to pre-approved venues that meet standards for pricing, reliability, and resilience.

Q26. 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?

51. Several additional risks may arise when an intermediary trades on its own account while also executing client orders:
    1. **Misuse of client funds for proprietary trading:** An intermediary may commingle client funds with its own trading portfolio to maximise internal profits without the client's knowledge. This could enable the intermediary to offload losses or volatility-related risks onto the client. The intermediary may trade on its own account using non-public client data or use its position to influence market dynamics, bringing fore the risks of market manipulation, price manipulation and front-running.
    2. **Evasion of KYC/CDD obligations:** An intermediary might blend client funds with its own investments to bypass Know Your Customer (KYC) and Customer Due Diligence (CDD) requirements under the CATP, particularly those concerning the origin of funds. This risk is heightened if multiple intermediary layers are involved before direct onboarding with the CATP, further obscuring the true source of funds and the identity of ultimate beneficiaries.
    3. **Biased investment recommendations:** An intermediary may provide independent investment while also selling in-house or affiliated products. This creates a risk that advice becomes biased toward products that generate higher commissions or fees than those that best meet the client's needs.
52. Some mitigations for the above currently used in Trad-Fi include:
    - Segregation of proprietary trading and exchange activities.
    - Segregation of advisory services, research, and sales.
    - Disclosures of proprietary trading activities.
    - Real-time trade surveillance (scenario based) with alerts being followed up and escalated.
    - Advanced analytics to monitor trade/ execution patterns.
    - Communications surveillance with alerts being followed up and escalated.
    - Periodic audits and Compliance oversight & testing.
    - Independent risk management periodic reviews.
    - Comprehensive record keeping and audit trail.
    - Full disclosure of potential conflicts of interest
    - Policies and Procedures: identifying, managing, and reporting conflicts (conflicts register).

Q27. 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.

53. Pre-trade transparency (the public disclosure of bid/ask prices and associated volumes before a trade executes) enhances market integrity, efficiency, and investor protection.

- **Retail investors:** Pre-trade transparency can significantly benefit retail investors by improving price discovery, enabling more informed decision-making, and increasing trust in market fairness. It helps retail clients assess whether pricing is competitive, reducing their exposure to information asymmetries. The most useful forms include aggregated order book depth across execution venues—though complex and costly to implement—and top-of-book quotes (best bid/offer and available volumes), which are more feasible and cost-effective. Costs to firms for providing such data could potentially be offset through commissions or fees charged to retail clients.
- **Institutional Investors:** Pre-trade transparency supports institutional investors by enabling more effective venue selection and smart order routing based on displayed liquidity. The most valuable tools include full-depth order books and advanced analytics that track real-time liquidity trends. These capabilities require high-quality data, along with substantial investment in data processing, cleaning, storage, and scalable infrastructure. As a result, costs may be significant, but could be mitigated by relying on specialised data providers rather than each institution building its own data aggregation systems.
- **Algorithmic traders:** Pre-trade transparency benefits algorithmic traders by providing a clearer view of market positioning, enabling rapid adjustments to spreads or order sizes, and facilitating the identification of arbitrage opportunities. Low-latency data feeds and real-time pre-trade data are essential for these strategies. However, this requires significant investment in robust, high-performance infrastructure, along with ongoing capital outlay to maintain and upgrade cutting-edge technology.

Q28. 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.

54. Post-trade transparency is important to mitigate systemic risk, promote market integrity and stability and promote investor confidence and protection. A balanced approach is required to ensure compliance costs and operational challenges do not stifle innovation.

55. Two potential alternative solutions to post-trade transparency requirements:

1. Centralised Crypto Trade Repositories

56. Establish a central post-trade repository where intermediaries report trades in real time or end-of-day.

57. This model enhances market surveillance, record-keeping, and transparency, providing regulatory oversight with consistent and comprehensive systemic data. It promotes uniform data usage and reporting and helps reduce information asymmetry between retail and institutional participants. Requiring data to be anonymised before inclusion in a central repository supports data privacy, though it introduces additional data management costs and complexity.

58. The centralised repository model is likely to involve high setup and ongoing maintenance costs. Firms would also need to invest in data aggregation, cleaning, processing, and secure storage. Additional cost drivers include ensuring compliance with data sharing and privacy requirements—particularly across borders—as well as implementing robust cybersecurity measures and business continuity planning. Smaller firms may face proportionally higher burdens due to limited resources.

2. Public Blockchain-Based Trade Recording (On-chain Transparency)

59. Recording trade confirmations or settlements on a public blockchain can enhance transparency and auditability, providing a tamper-evident record of transactions. This approach enables direct visibility for both the public and regulators, supporting more effective oversight.

60. The model may be less costly to establish compared to a centralised depository. However, firms could face ongoing transaction fees and costs associated with maintaining and

updating the system. There may also be complexity in designing the infrastructure to accommodate a wide range of asset classes, and questions remain over how quickly the system could be adapted to support new asset types as they emerge.

Q29. 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?

61. While transparency is essential to uphold market integrity, a tiered transparency model based on a risk-based approach may be considered.
62. Risk criteria could include factors such as financial exposure, market impact, and investor risk. For example, utility tokens used for non-investment purposes may require less oversight than more speculative or systemically significant assets.

CHAPTER 4 – CRYPTOASSET LENDING AND BORROWING

Q33. 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?

63. We agree with the risks that the FCA has summarised and agree that lending and borrowing should not be made available to retail customers at this time. In addition, if retail customers were to invest through intermediaries/wider investment portfolios, our concern would be that they may not be aware that their funds are being lent, as this will be done via the institutional carveout.

Q40. 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?

64. From a public interest perspective, a carefully structured exemption for qualifying stablecoins within cryptoasset lending and borrowing models could be both proportionate and effective.
65. Qualifying stablecoins are designed to maintain a stable value relative to fiat. Lower volatility materially reduces the risk of margin call (for borrowers); collateral liquidation (for lenders) and market-driven value loss (borrowers and lenders).
66. Unlike unbacked cryptoassets, qualifying stablecoins will be subject to FCA prudential, safeguarding, and conduct rules (once finalised). This adds a layer of systemic and consumer protection that does not currently exist in traditional crypto lending.
67. A blanket ban could unintentionally stifle innovation or push responsible lending activity into unregulated offshore channels. A narrow exemption for low-risk products maintains flexibility while mitigating harm — aligned with the FCA's duty to promote effective competition and international competitiveness under Financial Services and Markets Act 2023 (FSMA 2023).
68. Restricting lending/borrowing to well-defined stablecoins may improve transparency. Consumers are more likely to understand the risks, terms, and value stability of the assets involved — helping mitigate the FCA's concerns around complex, opaque products.
69. Suggested guardrails to ensure that the exemption is meaningful without undermining the core protections:
    - Only allow lending/borrowing where both the loan and collateral involve qualifying stablecoins.
    - Ban the use of platform tokens or unregulated cryptoassets as reward, fee, or collateral instruments in these models.
    - Impose caps on the size or term of such retail-facing loans, to avoid systemic build-up.
    - Apply Consumer Credit sourcebook (CONC)-style obligations (creditworthiness, forbearance, disclosure) to the models, tailored for stablecoins.

- Regulatory clarity is also needed on how retail customers would be protected, if they borrow or lend stablecoins, in scenarios where the issuing firm collapses, the stablecoin's value fluctuates, or the issuer or borrower lacks sufficient fiat reserves to support retail customers.

CHAPTER 6 – STAKING

Q42. 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?

70. While we believe that firms should be held accountable for preventable operational/ technical losses borne by retail customers (and note its alignment with the EU's Digital Operational Resilience Act (DORA)), we caution that the potential scope of such a requirement needs greater specificity, in order to provide greater legal and regulatory certainty for firms and consumers. A framework is needed that sets out the types of operational and technological failures in scope and the regulator's interpretation of loss events that are "preventable".
71. For example, where firms demonstrate strong compliance with any forthcoming operational resilience regime leading up to and at the time of the operational incident, would this support the grounds for the event being "unpreventable"?
72. We note some confusion in the DP in respect of which incidences will be caught by the requirement. Paragraph 6.12 indicates that firms will need to compensate consumers for losses which occur as a result of the actions of third-party technological providers. However, 6.14 sets out "we do not propose to extend accountability to the firms to include incidents that happen outside of their control, such as blockchain disruptions". We would welcome clarity in defining events which are outside of a regulated firm's control, as these may involve third parties and may occur despite the best efforts to ensure operational resilience within their ecosystem.
73. It will be important to communicate the nuances of this requirement with retail consumers, prior to entering into staking activities. There is a risk that they interpret the requirement to cover losses as covering all incidences. Further, they may see it as a blanket requirement in respect of all losses that they incur in respect of their holdings, including where losses have been derived through price movements.
74. We would encourage the regulator to consider the wider impact to regulated firms, should they need to hold significant capital, in order to provide staking services. The majority of unbacked crypto activities to date, rely on price appreciation to generate value for holders. Staking is a means by which holders of crypto assets might generate additional returns. Higher capital requirements are likely to result in fewer firms offering the service, which ultimately might be at the cost of retail consumers looking to generate value from their holdings.
75. These requirements may also significantly impact upon the ability of regulated firms to obtain business interruption insurance if risk coverage has to cover potential consumer losses.
76. The following alternative proposals can be considered in instances where a firm cannot fully absorb the loss or full loss absorption is deemed disproportionate:
    1. Slashing insurance coverage (mandatory or opt-in);
    2. Risk-tiered staking models with disclosures: consumers select between lower-risk (insured/firm-managed) or higher-risk (uninsured) staking products;
    3. Slashing reserve buffers as part of capital requirements; and
    4. Retail compensation schemes for operational failures (similar to FSCS-type principles, if scaled to market).

Q43. Do you agree that we should also rely on the operational resilience framework in regulating staking, including the requirements on accountability?

77. The FCA's existing framework under Senior Management Arrangements, Systems and Controls Sourcebook (SYSC) 15A (Operational Resilience) already requires:
    - Identification of important business services
    - Impact tolerance setting and mapping of resources (people, tech, facilities)
    - Scenario testing and communication plans
78. Staking – especially pooled or delegated – would fall under the scope of important services when it affects client asset custody, validator performance, or slashing risks. The framework rightly places accountability on firms for their technology, governance, and third-party dependencies.
79. Unlike DORA, which is highly prescriptive, the FCA approach provides room for proportional compliance based on the firm's size and complexity — suitable for a developing market like cryptoassets and staking.
80. There are a few areas where adoption from DORA may be useful:
    A. **Third-party validator risks:** The FCA could codify expectations for due diligence, risk sharing, and contractual controls with validator-as-a-service providers — similar to DORA's mandatory oversight and contractual clauses for critical ICT providers.
    B. **Incident classification and reporting:** DORA sets reporting timelines and thresholds for major incidents (within hours). FCA's approach is more flexible but less time bound. Retail staking platforms may need faster notifications when rewards are missed or slashing occurs.
    C. **Audit and insurance expectations:** DORA includes mandatory audit rights and resilience testing for critical ICT providers. The FCA could require regulated staking firms to include auditability and resilience clauses in smart contract and validator service arrangements.
81. It is also important to consider the operational resilience of critical third-parties as well and the regulator should consider extending the requirements of the Critical Third Parties Sourcebook to staking firms should any of the organisations involved in staking become systemic to the financial system.
82. We believe that this should encompass any means of exploiting deficiencies, including within the software, resulting in any loss while the third party is engaged. However, this should not extend to disruptions on the blockchain or for events that are reasonably outside of their control.

Q44. 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?

83. We agree that firms (direct and intermediaries) should get consent from retail consumers covering the value and type of assets to be staked.

Q47. 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?

84. We agree that regulated staking firms should be required to segregate staked client cryptoassets from other clients' cryptoassets. However, it is worth considering whether there exists, or will exist in the near future, an equivalent to a Title Transfer Collateral Arrangement (TTCA) for staked cryptoassets.
85. There are several possible client asset segregation arrangements:

1. **Individual wallets** – would ensure high level of segregation but come with significant wallet / key management requirements.
2. **Omnibus wallet** – pool of staked client assets held in a single omnibus wallet, but internal records are maintained to track each individual clients' holdings. Cryptographic proofs or other verification methods could be used to demonstrate client ownership. If possible, it may be practical to maintain a segregated omnibus wallet, per staked cryptocurrency.
3. **Smart contract** – smart contracts with predetermined outcomes are used to track client-specific allocations within a pooled staking arrangement, releasing funds or allocating awards upon criteria of validating being met.

86. Similar to the transparency on use of wallets, firms should clearly define the terms and conditions in client agreements regarding asset segregation. This sets expectations and provides legal clarity on how assets will be managed.

Q48. Do you agree that regulated staking firms should be required to maintain accurate records of staked cryptoassets? If not, please explain why?

87. We agree that regulated staking firms should be required to maintain accurate records of staked cryptoassets, consistent with existing CASS requirements where possible.
88. As highlighted by ICAEW's 2024 publication; Consideration For Auditing Cryptocurrencies; under management competence and responsibility (page 10): similar to the existing CASS rules, regulated staking firms should be required to maintain accurate books and records of any staked assets and rewards that are due to clients, with sufficient controls in place to ensure these books and records are kept up to date in line with real world movements.
89. In addition, it may be necessary to take into account whether there are any intermediaries in the staking process.
90. Prior to staking, firms should obtain express consent from retail clients for the conditions in which the firm is holding the client's cryptoassets, e.g., the amount of cryptoassets staked, conditions for payment or return of cryptoassets, as well as fee-charging arrangements imposed by the firm. The firm should also send retail clients key information on staking products and the associated risks before they stake a client's cryptoassets.

Q49. 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?

91. We agree that regulated staking firms should conduct regular reconciliations of staked cryptoassets. This is essential to ensure client asset protection, operational integrity, and regulatory compliance — particularly given the custodial and technological risks unique to staking business models.
92. Regular reconciliations bolster consumer protection by ensuring firms hold the correct quantity of staked assets on behalf of each client; that rewards and slashing penalties are accurately reflected in client balances; and that there are no unaccounted shortfalls or surpluses, which could otherwise result in losses for consumers.
93. Accurate tracking of stake amounts and validator allocations ensures fair and transparent distribution of staking rewards, particularly in pooled or liquid staking arrangements.
94. Reconciliations reduces operational risk management by increasing the oversight in the detection of wallet misconfigurations, validator errors, or slashing events and providing back up in case of insolvency, hacking, or client disputes.
95. This mirrors expectations for custody providers under the CASS and emerging crypto safeguarding rules — supporting market integrity and cross-regime consistency.
96. Recommended frequency is driven by various factors including understanding nature of the entity (as highlighted by ICAEW publication; Consideration For Auditing Cryptocurrencies; under understanding entity (page 4)) or volume of transactions.

97. As crypto operates 24/7, an appropriate reconciliation frequency is likely to be higher than the monthly minimum suggested by current CASS rules and more likely to be daily reconciliation for firms with large volumes or real-time staking operations and a weekly minimum for all other firms, with flexibility to scale based on factors such as number of clients and staked assets; use of third-party validators; and the complexity of staking models (e.g. liquid staking vs native staking).
98. This is consistent with the principle of proportionality under the FCA's supervisory approach.
99. The frequency may also depend on the blockchain they are staking on since each blockchain has its own protocol that dictates how often reconciliations should occur. Some networks may have real-time reconciliation, while others might do it at set intervals (e.g., daily, weekly, or after specific blocks are validated).
100. Blockchain helps reconciliations for staking firms through all its known benefits - immutable and transparent records; programmable logic (smart contracts) and real-time access.
101. But there are complications to consider as well in the use of blockchains for reconciliation:
    1. **Custody Disaggregation**: when staked funds are pooled across clients in omnibus wallets or third-party validator accounts, it becomes hard to map who owns what share of the stake how much of each reward/slash belongs to whom.
    2. **Off-chain Abstractions**: some staking platforms (especially custodial or CEX-led) abstract the on-chain logic: firms may issue internal IOUs ("I Owe You") instead of tracking actual stake. This increases reconciliation complexity and legal ambiguity.
    3. **Variability Across Blockchains**: each blockchain has its own i) reward payout intervals; ii) unbonding periods (e.g. 7 days vs 21 days); and iii) validator structures and slashing logic. This variability fragments operational processes and requires bespoke tooling and logic per chain.
    4. **Limited Metadata On-Chain**: blockchains do not natively track client identity or allocation. Without robust internal ledgers, firms cannot match public staking balances to individual clients — leading to reconciliation gaps.
102. There are also platforms with features that make reconciliation harder. Such platforms typically exhibit:
    - Pooled custody with no sub-accounting (e.g., certain exchanges);
    - Liquid staking protocols (e.g. Lido, Rocket Pool);
    - Involve tokenized claims (e.g., stETH), which does not map 1:1 with real-time on-chain stake due to rebasing and slashing;
    - Require reconciliation between synthetic (token) layer and native (validator) layer;
    - Validator-as-a-service providers with limited reporting transparency; and
    - Blockchains with frequent state changes and complex delegation logic (e.g. Cosmos zones with redelegation).

CHAPTER 7 – DEFI

Q50. 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?

103. We agree that the FCA's proposed approach — applying activity-based regulation to centralised DeFi services and supporting compliance through guidance — is proportionate and forward-looking.
104. We support the principle that "same risk, same regulatory outcome" should apply to cryptoasset activities regardless of the technology used. This is consistent with international

standards (e.g. The International Organization of Securities Commissions (IOSCO)'s DeFi policy recommendations) and avoids regulatory arbitrage.

105. However, prescriptive rules may be ineffective or inapplicable in truly decentralised contexts. Therefore, issuing clear, practical guidance to help identify when DeFi activities fall within the regulatory perimeter is the most appropriate first step.

106. We also welcome the FCA's intention to host a stakeholder forum, which is essential to ensure the emerging regime remains technically relevant and adaptable to innovation in protocol governance, smart contracts, and Decentralised Autonomous Organisation (DAO)-based infrastructure.

107. Emerging industry practices that enable greater compliance readiness among DeFi participants include:

    a) **DeFi Front-End Entity Structuring:** Increasingly, DeFi protocols are paired with regulated or incorporated legal entities that handle front-end interfaces (e.g. wallets, web apps), which can be subject to AML/CFT, consumer protection, and complaints handling rules. For example, DeFi projects establishing UK-registered entities to oversee UI/UX and apply basic KYC controls.

    b) **Permissioned Protocol Layers:** Some DeFi protocols now implement allow-list functions for specific actors (e.g. validators, liquidity providers) or jurisdiction-based restrictions using wallet-level geofencing and compliance modules.

    c) **Code Transparency and Auditability:** Industry leaders increasingly publish third-party audit reports, commit to open-source codebases, and maintain public bounty programs to encourage external security review.

    d) **DAO Governance Disclosures:** More decentralised protocols are introducing structured disclosures about governance, including voter concentrations, proposal thresholds, and admin key controls.

    e) **Transaction Monitoring & Risk Scoring APIs:** Front-end providers may integrate chain analysis tools (e.g. TRM, Chainalysis) to score wallet risk and implement real-time screening for sanctioned addresses or abnormal flow patterns.

108. Specific measures that can be implemented to mitigate the risks posed by DeFi services to retail consumers include:

    - Consumer warnings and disclaimers on interfaces that interact with unaudited or experimental DeFi protocols.
    - Voluntary opt-in disclosures describing the role of smart contracts, absence of fiduciary duties, and risk of loss from Oracle manipulation or code vulnerabilities.
    - Integration with regulated stablecoins or custodial off-ramps, ensuring that fiat entry and exit points are AML-compliant and supervised.
    - Risk scoring of smart contracts and token pools, based on concentration of governance rights, immutability of contracts, and quality of Oracle feeds.
    - Segregation of front-end (UI/UX) operations from protocol layer governance, allowing clear assignment of liability and regulatory expectations.

109. We support the FCA's guidance-led, activity-based approach to DeFi and recommend building regulatory capacity around three pillars:

    - Perimeter clarity through use-case examples and DAO governance thresholds;
    - Proportional compliance tools (e.g. front-end standards, safe harbour disclosures); and
    - Industry engagement via sandbox initiatives or technical consultation panels.

110. This measured approach can ensure retail users receive appropriate protection without undermining DeFi innovation or its benefits for financial inclusion, resilience, and transparency.