18 November 2026

CryptoUK
Formal House
60 St George's Pl
Cheltenham GL50 3PN

Submitted by email: GC26-7@fca.org.uk

Dear FCA

Response to: (GC26/7): Decentralised Finance (DeFi) (the "*Guidance Consultation*")

CryptoUK ("**we**") and its members welcome the opportunity to respond to the FCA's Guidance Consultation on its proposed non-Handbook guidance on Decentralised Finance ("**DeFi**"), which explains how existing operational resilience requirements under SYSC 15A, financial crime requirements under SYSC 6 and the Money Laundering Regulations (the "**MLRs**") may apply where firms interact with, facilitate access to, or provide financial services using DeFi.

CryptoUK is the UK's self-regulatory trade association representing the cryptoasset sector. Our members comprise over 150 of the leading companies across the sector and across the UK. Many of our members are also international and engage with regulators and policy frameworks on a global basis.

We have provided detailed answers to each question posed in the Guidance Consultation within the Appendix. We seek to offer pragmatic and relevant observations about, and suggestions in response to, the content within the Guidance Consultation. However, at the outset, we would like to make a number of general comments as follows:

Our central recommendation is that obligations reflect the relevant activity and the person's actual authority, custody, discretion and control. Publishing software, participating in governance and operating a financial service are distinct functions. Put simply, regulation should attach to the activity carried on and the outcome it produces for consumers and markets, not to the technology through which it is delivered. The same underlying technology can support many different activities, some regulated and some not; regulating the technology itself risks capturing lawful, purely technical functions without better addressing the outcomes that matter. Institutions using public protocols remain responsible for applicable compliance, customer protection and fiduciary duties, including applicable best execution requirements.

<u>Scope and relationship to perimeter guidance</u>

We welcome the statement in draft paragraph 1.11 that GC26/7 creates no new requirements, and the distinction in draft paragraph 1.12 between "must" (an existing requirement) and "should" (guidance). We ask that the FCA reinforce this throughout the examples and distinguish legal duties from optional emerging practices. Each example should identify its assumed regulatory basis and which service creates the relevant obligation. Consistent with draft paragraphs 2.2 and 2.3, the use of software, smart contracts or DLT should neither by itself determine that an activity is regulated nor by itself attract

additional obligations. Financial crime guidance should not become an alternative route to expanding the perimeter.

We request consistency with CP26/36, including its proposed technical services guidance. The absence of custody does not resolve every UK perimeter question: arranging, dealing and other activities require their own analysis, as does the application of the MLRs and the financial promotions regime (see draft paragraph 2.2). Our recommendations seek protection for genuinely technical functions within the applicable statutory framework, with legislative changes considered where guidance cannot deliver that result.

Yours sincerely

Nick Brooks
Policy Director, CryptoUK

Appendix

Guidance Consultation Questions:

1. **Do you agree with our description of the operational resilience risks that may arise when firms provide financial services using DeFi? If not, please explain why.**
   We broadly agree with the description of operational resilience risks in draft paragraphs 3.7–3.11, and that firms should assess material risks from protocol dependencies and failures. Building on the risk categories in the table following draft paragraph 3.11, the final guidance should distinguish vulnerabilities in code from risks arising through integration, privileged access and a firm's own service design. A firm should base its assessment on how a protocol actually operates and is integrated into its service, rather than on how the protocol is described or whether its source code is public.

   The risk table following draft paragraph 3.11 notes that publicly available smart contract code can allow vulnerabilities to be identified and exploited. We ask the FCA to recognise that open-source review, independent verification and diverse infrastructure can also improve resilience. Firms should assess code quality, review coverage, remediation history and dependency concentration. For clarity, we would welcome confirmation that public availability of code is not, in itself, treated as evidence of deficient security.

   The guidance should also recognize the trade-off between immutable execution from concentrated administrative control. An emergency key can mitigate an exploit, but can itself be compromised or misused. Conversely, removing intervention powers can limit unilateral changes, but also limits the response available during an exploit. We would welcome confirmation that neither design is presumed more compliant, and that firms should instead assess the trade-offs against their service, customer commitments and available mitigations.

2. **Do you agree with our proposed guidance on how firms should assess and manage those operational resilience risks? Are there other risks or emerging practices we should consider?**
   We support proportionate assessment and testing of the services regulated firms deliver, and welcome the statement in draft paragraph 3.20 that the important business service is the service delivered to the client rather than the underlying technology or protocol. For draft paragraphs 3.14–3.42, we ask the FCA to confirm, consistent with draft paragraph 3.39, that firms can achieve resilience outcomes in a number of ways, including those described below, without obtaining control over an independent public protocol.

   Assess dependencies using evidence firms can obtain
   A firm should document the protocol versions and addresses it uses, relevant upgrade and administrator powers, oracle and bridge dependencies, and material concentration across infrastructure providers. Assurance may draw on independent audits, verified code, public governance records, testing and observed performance. An audit is evidence of review, not a guarantee against loss; firms should assess its scope, age and unresolved findings.

We ask the FCA to clarify how these sources can support due diligence where no operator exists to sign a contract, grant private audit rights or provide a service-level agreement. Assessments should also distinguish a public protocol dependency from a contractual outsourcing relationship (see draft paragraph 3.41) while preserving the firm's responsibility for managing the risks of its chosen service.

Test feasible responses and disclose their limits

Testing should examine disruptions affecting the firm's service, including oracle manipulation, bridge failure, loss of infrastructure connectivity, compromised signing interfaces and unexpected changes to privileged access. Firms should consider whether dependencies thought to be independent share the same underlying provider or failure mode.

Responses a firm might test against these scenarios include limiting new exposure, using alternative connectivity, issuing client alerts and supporting recovery where technically feasible. Switching protocols or withdrawing assets can create additional execution, liquidity and security risks. Firms should test those assumptions rather than treating an exit plan as necessarily available during stress.

We do not seek relief from applicable impact-tolerance requirements, and we recognise, as draft paragraph 3.13 notes, that resilience measures cannot prevent every disruption. We ask instead that the FCA explain how firms can evidence compliance where they cannot pause, reverse or repair an external protocol, and when residual risk makes a proposed service unsuitable. We would also welcome confirmation that firms are not expected to redesign permissionless infrastructure to introduce central intervention powers. We further ask the FCA to explain how the guidance that firms should work with third parties to ensure the validity of scenario testing (draft paragraph 3.32) applies where the dependency is a public protocol with no counterparty.

Clarify the noncustodial wallet example

The Firm B examples at draft paragraphs 3.29 and 3.34 describe a firm that provides a number of regulated financial services as well as access to DeFi through a noncustodial wallet. We ask the FCA to specify which of those regulated activities and important business services bring Firm B within SYSC 15A, to explain how its wallet dependencies (such as the oracles, DEX aggregators and RPC node providers referred to in those examples) affect those services, and to confirm that the example does not suggest that supplying noncustodial wallet software alone requires authorisation or makes every wallet function a regulated service.

Protect security work throughout the software lifecycle

We welcome draft paragraphs 1.9 and 2.3, which confirm that the use of software, smart contracts or DLT does not by itself determine whether an activity is regulated. We ask the FCA to confirm, in the operational resilience context and consistently with the statutory tests, that writing, publishing, deploying, maintaining or auditing noncustodial code does not by itself establish that a person operates the underlying financial service. This should cover good-faith vulnerability disclosure, bug bounties and security improvements, the value of which Case Study 2 illustrates. The assessment should examine any retained operational powers and services actually

performed; a contribution to software should not alone transfer an integrating firm's regulatory duties to its developer.

3. **Do you agree with our description of the financial crime risks that may arise when firms provide financial services using DeFi? If not, please explain why.**
We agree that firms must address fraud, illicit finance and sanctions risks relevant to their activities. The description in draft paragraphs 4.4–4.11 should distinguish legitimate technological functions from the circumstances in which criminals exploit them. This would produce more useful risk assessments and reduce indiscriminate restrictions on lawful activity.

   For draft paragraphs 4.8 and 4.19, we ask the FCA to clarify that self-custody, privacy-enhancing technology or use of interoperable protocols does not alone establish suspicious activity or necessarily require enhanced due diligence. Firms should consider purpose, transaction behaviour, available attribution and other relevant evidence, alongside any mandatory legal triggers. The privacy that these technologies provide can also protect consumers and businesses from surveillance, fraud and targeted attacks.

   The final guidance should also recognise the investigative value of public transaction records. Firms can use blockchain analytics to identify relationships and patterns, with appropriate attention to attribution uncertainty and false positives. Indicators should support an assessment of the facts rather than automatically determine a customer's treatment.

   For the discussion of fragmented responsibility across developers, governance participants and infrastructure providers (under "Intermediary and control gaps" in the table following draft paragraph 4.10), we ask the FCA to distinguish technical involvement from responsibility arising under applicable law. A gap in an intermediary-based compliance model does not, by itself, establish that a software contributor or token holder has become an obliged entity.

4. **Do you agree with our proposed guidance on how firms should assess and manage those financial crime risks? Are there other risks or emerging practices we should consider?**
We support risk-based controls for firms subject to the relevant requirements. Draft paragraphs 4.12–4.28 should explain how those firms can manage exposure to open networks while preserving lawful self-custody and minimising unnecessary collection of personal information.

   <u>Assign controls to the relevant activity</u>
   A regulated intermediary should assess its customer relationships, products and transaction flows, carry out required due diligence, maintain appropriate monitoring, and meet applicable reporting and sanctions duties. Using DeFi should not displace those obligations. Equally, a firm's decision to integrate software should not impose those duties on an independent developer that performs no relevant regulated or obliged activity.

   <u>Assess indirect exposure in context</u>
   For draft paragraphs 4.15, 4.19 and 4.23, we ask the FCA to explain how firms should evaluate indirect connections to illicit activity. Relevant considerations include the

reliability of attribution, proximity, timing, value, transaction pattern and the possibility of unsolicited transfers. A wallet's interaction with a widely used pool should not alone be treated as proof of wrongdoing or an automatic basis for refusing service.

Firms should document escalation and review procedures, including how they resolve disputed or stale analytics labels. These recommendations would not override an applicable prohibition, asset-freeze requirement, enhanced due diligence trigger or reporting duty. The guidance should distinguish risk indicators from the legal tests that require a particular action.

Recognise privacy-preserving compliance tools

The FCA should recognise verifiable digital credentials, selective disclosure and zero-knowledge proofs as potential tools for meeting specified compliance needs. For example, a credential may help establish an eligibility attribute without exposing unrelated personal information. Such tools should be assessed against the particular legal requirement; they do not automatically replace required identification, verification or recordkeeping.

Useful guidance would address issuer assurance, credential validity and revocation, fraud resistance, auditability and lawful access to retained records. Firms should minimise the information collected and avoid placing personal identity data on public ledgers. More data collection can create additional cybersecurity risks without necessarily improving detection.

Make Travel Rule expectations workable

For draft paragraphs 4.26–4.28, we ask the FCA to distinguish transfers involving another obliged provider from those involving a self-hosted wallet, and to explain the information and risk assessment expected from the regulated firm in each case, including how it can obtain required information from its own customer under Regulation 64G of the MLRs where appropriate. The guidance should not imply that every wallet or smart contract has a compliance officer or a counterparty messaging endpoint.

Technical implementation guidance should address missing information and interoperability without creating a general requirement to identify every participant in a public liquidity pool or every downstream holder of an asset. Firms must still comply with applicable transfer-information and recordkeeping requirements. We request examples separating those requirements from additional measures considered on a risk-sensitive basis.

5. **Are there other risks or emerging practices related to DeFi which we should consider?**

The FCA should include examples addressing vaults and distributed governance. In a vault arrangement, identify separately the software author, a curator selecting eligible markets, a manager with allocation discretion, the interface provider and the user. A curator or manager with continuing authority over strategy or assets may require a different assessment from a developer supplying reusable code. Neither the "vault" label nor receipt of a fee should substitute for examining the activity and relevant statutory test.

Governance analysis should examine voting concentration, delegated powers, upgrade execution, emergency authorities and the ability to coordinate binding decisions. Holding a governance token or casting a vote should not alone establish that a participant operates a financial service. A narrowly limited emergency role should be evaluated according to its actual powers, while substantive control retained through a committee or related persons should receive appropriate scrutiny.

The FCA should also recognise transaction simulation, independent verification of signing details and responsible vulnerability disclosure as useful practices. Firms should assess these tools against their actual service risks. No particular audit, governance structure or security product should become a universal compliance condition through an illustrative example.

6. **Are there other steps that could be taken to reduce financial crime risks in DeFi? Are there other regulatory measures that we should consider to reduce the financial crime risks in DeFi?**
We recommend practical measures that improve detection and accountability while preserving lawful access to decentralised systems.

Provide coordinated implementation examples
The FCA should work with relevant UK authorities, including HM Treasury, HMRC and the Bank of England, and with industry to publish examples distinguishing regulated intermediation, technical access and direct user activity. Examples should cover institutional protocol use, wallet software, interfaces, vault management and limited governance roles. They should identify the activity and legal basis before discussing the controls expected of an obliged firm. This would help prevent both under-compliance and unnecessary withdrawal of useful services.

These examples need to reflect how DeFi transactions are actually executed. Members' experience is that illustrative DeFi transactions used in recent consultation and engagement have oversimplified how such transactions work. For example, a single user transaction may in practice route through a wallet, an interface, an aggregator, several smart contracts, oracles and bridges, each potentially involving different persons and different activities. Where that complexity is not represented, the resulting analysis is less effective, and industry has had to prepare its own examples in response. We would welcome the opportunity to work with the FCA to develop technically accurate worked examples.

The need for accurate examples extends beyond the FCA. Many different activities, with different regulatory characterisations, can take place on the same underlying technology. There is a difficulty with characterising DeFi activity correctly and this shows that there is value in coordinated, technically accurate examples across authorities, so that the regulatory, tax and accounting treatment of the same arrangement is analysed consistently and by reference to the activity carried on rather than the technology used.

Support targeted information sharing and testing
Authorities and firms should develop timely channels for sharing verified exploit indicators and fraud typologies, subject to applicable privacy and confidentiality safeguards. Shared information should include provenance and correction mechanisms so that inaccurate labels do not propagate unchecked. Technical testing

of credential systems, analytics and transfer-information interoperability could identify what improves detection and what adds friction without a corresponding benefit.

Recognise documented good faith compliance efforts

Within its lawful discretion, the FCA should explain how it will consider proportionate, documented controls, prompt remediation and cooperation when assessing a firm's response to a novel DeFi risk. A subsequent exploit or third-party misuse should not, by itself, establish that a firm's earlier risk assessment was inadequate. This request is for supervisory clarity and does not seek immunity for misconduct or displacement of statutory duties.

Review practical effects after implementation

We ask the FCA to monitor whether the guidance improves detection and resilience, and whether its application produces unnecessary exclusion of self-hosted wallets, privacy tools or open-source infrastructure. It should revisit examples as technology and evidence develop and assess material implementation burdens before turning emerging practices into prescriptive expectations.

Clear boundaries and proportionate expectations would allow institutions to use DeFi responsibly while supporting innovation in noncustodial infrastructure. We appreciate the FCA's consideration of these recommendations.

About CMS

CMS is a leading international law firm that provides full service legal and tax advice to the world's major financial institutions. With 78 offices in over 40 countries and more than 5,000 lawyers, CMS has long standing expertise in its local jurisdictions and can powerfully leverage the CMS network on cross border mandates. Our UK Financial Services team regularly advises the leading global investment banks, fund managers, intermediaries, market makers and institutional investors on technical regulatory and transactional matters. Many of our team have spent time inhouse at our clients or at the regulators and we seek to develop productive working relationships with our clients and prioritise practical, business driven solutions. Further information is available at www.cms.law.

Key contact:

Sam Robinson – Partner, Financial Services Regulatory, sam.robinson@cms-cmno.com

Yasmin Johal – Senior Associate, Financial Services Regulatory, yasmin.johal@cms-cmno.com

Marelize Abercrombie – Associate, Financial Services Regulatory, marelize.abercrombie@cms-cmno.com