



The BBA CLG Ltd, Kemp House  
124 City Road  
London, EC1V 2NX, UK

22 October 2026

Financial Conduct Authority  
Crypto Policy  
Payments & Digital Assets Division  
12 Endeavour Square  
London, E20 1JN

For submission by email to: [GC26-7@fca.org.uk](mailto:GC26-7@fca.org.uk)

## **Response to FCA Guidance Consultation GC26/7: Decentralised Finance**

*(Consent to publication: The British Blockchain Association (BBA) consents to publication of our name as a respondent. We are responding as an organisation and do not request confidential treatment for this submission.)*

### **Introduction and Summary of Position:**

The British Blockchain Association (BBA) is one of the UK's longest-established blockchain industry bodies, founded in 2017. We advance the evidence-based adoption of blockchain and distributed ledger technologies, serve as Secretariat to the All-Party Parliamentary Group on Blockchain Technologies, and co-authored the UK's National Blockchain Roadmap (Vision 2030). Our institutions include the Centre for Evidence-Based Blockchain (CEBB), the Journal of the British Blockchain Association (JBBA) and the Blockchain Associations Forum (BAF).

In this response, "we", "us" and "our" refer to the British Blockchain Association (BBA).

We support the FCA's proposed guidance on operational resilience and financial crime risks in DeFi. It creates no new requirements. [5] We welcome its distinction between "must" and "should" (draft guidance, paragraph 1.12), its recognition that technology alone does not determine the perimeter (1.9), and its cross-references to PS26/18 and CP26/36 (1.16 and 2.1-2.3). The consultation introduction also asks firms to identify applicable requirements (paragraph 1.4, page 2). [5, 6, 15]

Our support is qualified. The guidance should apply these distinctions consistently, explain compliance where firms cannot alter a protocol, and apply financial crime indicators proportionately. Public transaction records do not alone establish identity, lawful ownership or solvency. We answer all six questions below, propose corrections to the sanctions and Travel Rule passages, and address implementation costs and the conditions for useful DeFi services to benefit the UK.

**Question 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.**

## **Response**

### **Agreement and necessary distinctions**

1.1 We broadly agree with the description of risk. We would, however, separate four questions: whether the code executes correctly; whether the economic mechanism remains viable under stress; whether the firm can continue its service; and whether affected clients can obtain a remedy. A system can pass the first test and fail the other three. The final guidance should make those distinctions explicit.

1.2 Liquidity is a good example. Hafner and colleagues examine withdrawal risk on a new lending platform and analyse depositor concentration, including through the Herfindahl–Hirschman Index. Their Folks Finance case study supports measuring concentration and testing large withdrawals; it does not establish a generally safe concentration threshold. The authors disclose that all are affiliated with the use case. [1] We recommend that resilience testing combine withdrawal pressure with network congestion and deteriorating collateral liquidity. Testing a server outage alone would miss the circumstances in which customers most need access to their assets.

1.3 Economic assurance deserves its own treatment. Kampakis and Stankevičius propose a tokenomics audit framework and illustrate it through case studies, including a retrospective analysis of Terra/Luna. [2] This is useful support for examining incentives, assumptions and sensitivity to stress. It is not a substitute for a code review, and completing a checklist does not justify describing a product as safe. We recommend separate assessments of software integrity, economic design and operational dependencies, with the findings reconciled before approval.

1.4 Governance should be assessed through actual powers and how they are used. In a study of nine DeFi projects, Barbereau and colleagues found concentrated voting rights and low participation. [10] Those findings justify scrutiny of governance concentration; they cannot establish the position of every current protocol. A firm's assessment should identify who can upgrade contracts, change collateral parameters, replace an oracle, move treasury assets or disable an emergency control. It should also identify delegated votes, common control of signers and the practical cost of acquiring decisive influence. Case study 6 (Drift) shows why timelocks and pre-signed transactions belong in that assessment.

### **Risks requiring fuller treatment**

1.5 We recommend explicit scenarios for stale or manipulated oracle prices, a stablecoin losing its peg, failure of a bridge or sequencer, compromised transaction-signing interfaces, governance capture and disruption to liquidations. Testing should include combinations. Several apparently independent providers may rely on the same cloud infrastructure, data source or software dependency, so a count of providers is a poor substitute for a map of common failure points. The technical literature on DeFi composition supports examining dependencies across protocols. [11]



The BBA CLG Ltd, Kemp House  
124 City Road  
London, EC1V 2NX, UK

1.6 The distinction between technical and legal settlement also matters. A transaction recorded on a chain does not, without more, establish an enforceable claim against an off-chain asset or resolve insolvency priorities. We recommend that firms using tokenised assets document the issuer, governing law, redemption terms, custody arrangements and the consequences of insolvency, and assess these alongside the technical pathway rather than assume token ownership settles them.

1.7 Public code and transparent records can assist independent scrutiny. The final guidance should explain how firms may use those features as evidence, while requiring them to check the deployed contract address, implementation version and upgrade permissions. The draft notes that publicly available code can be studied by attackers (table at 3.11). That is true, but it should not be read as implying that open-source software is inherently less resilient than proprietary software. The relevant questions are the quality of assurance, maintenance, dependencies and response arrangements.

**Question 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?**

## **Response**

### **Preserve the statutory and regulatory boundaries**

2.1 We support applying existing resilience requirements to the services for which a firm is responsible. Paragraph 1.4 of the consultation introduction (page 2) rightly asks firms to identify the requirements that apply to them. We suggest the final guidance go one step further with a short applicability table separating firms already subject to SYSC 15A, firms that will become subject to it under the cryptoasset regime from 25 October 2027, and businesses with a different regulatory status. An MLR registration should not be presented as establishing that every Handbook provision applies; the underlying activity, permission and application provisions determine the answer.

2.2 We welcome the cross-references to PS26/18 and CP26/36. CP26/36 consults on guidance interpreting a proposed technical-services exclusion, which would be inserted as article 9Z2A of the Regulated Activities Order by draft regulations laid before Parliament on 15 September 2026. The exclusion would concern only arranging deals in qualifying cryptoassets. It would apply only where the provider is neither an authorised person nor a payment service provider and merely provides a technical service allowing access to the relevant regulated services of an appropriately authorised or exempt third party, or to a decentralised protocol. It would not provide a general exclusion for software or extend to other regulated activities. [6, 22] GC26/7 should apply these distinctions consistently: software development, a wallet interface or a connection to a public network does not, by itself, establish a regulated financial service. Equally, describing a commercial service as software cannot settle its legal character. We ask that the worked examples identify the precise regulated activity before applying controls, and that the final guidance be checked against the applicable legislation and final CP26/36 guidance.



The BBA CLG Ltd, Kemp House  
124 City Road  
London, EC1V 2NX, UK

2.3 The draft refers firms to FG26/6 on operational resilience for cryptoasset firms (paragraph 3.4). [16] The final DeFi guidance should state how the two documents fit together, so that firms are not left to reconcile overlapping expectations themselves. The evidence file we propose at 2.6 is intended to sit within that framework, not alongside it.

2.4 For firms within its scope, SYSC 15A.2.9R requires the ability to remain within the impact tolerance for each important business service during a severe but plausible disruption to operations. SYSC 15A.2.10G explains that firms should generally not achieve that outcome through steps that would breach another regulatory obligation, interfere with the proper exercise of a discretion conferred by a rule or regulation, or increase the risk of harm to clients, the soundness, stability or resilience of the UK financial system, or the orderly operation of financial markets. [7] We do not propose replacing that standard with a reasonable-efforts defence. The FCA should instead explain how firms can meet it through service design, limits, alternative delivery arrangements and realistic recovery plans. We recommend that, where compliance cannot be demonstrated, the service be changed, restricted or not offered.

2.5 Impact tolerance should not be equated with an ordinary uptime target or with the absence of any loss. We recommend measuring affected clients, loss of access, transaction integrity, exposure during liquidation delays and the duration of disruption. A notice on a status page does not remedy a failure to deliver the underlying service, and firms should not promise immediate redemption where the protocol has an unavoidable exit queue.

## **Evidence that should satisfy supervisors**

2.6 We propose a proportionate evidence file for each material DeFi service: the legal activity analysis; a diagram of relevant dependencies; the deployed code and configuration assessed; independent assurance findings and unresolved weaknesses; concentration and liquidity analysis; scenario results; incident responsibilities; and the decision to accept residual risk. Its depth should follow exposure and potential harm. This is a proposed supervisory approach, not a claim that the law currently requires a document in this form.

2.7 An audit should state its scope, date, methodology, tested version, exclusions and unresolved findings. A material upgrade should trigger a review proportionate to the change. Formal verification can establish specified properties under stated assumptions; it should not be presented as proving every aspect of economic or operational safety. Firms should assess auditor competence and conflicts, and explain why any continued reliance on an existing report is justified.

2.8 Emergency controls need a balanced assessment. A pause function can limit an exploit, but it also concentrates power and may block withdrawals. An immutable contract avoids discretionary alteration but can be harder to repair. We recommend requiring firms to explain the trade-off, identify who holds intervention powers and test their lawful use. The FCA should not turn a particular architecture, such as an administrator key or a mandatory pause function, into an implicit condition of operating in the UK.

2.9 The worked examples of Firm A and Firm B are helpful. We suggest adding three more: a staking service facing a protocol exit queue; a firm using an immutable lending pool; and an execution service whose primary network stops processing transactions. Each should



The BBA CLG Ltd, Kemp House  
124 City Road  
London, EC1V 2NX, UK

distinguish actions the firm can take from actions that require an issuer, validator or governance vote. An alternative interface is not a recovery route if it reaches the same failed network, and a contractual promise from a service provider is not evidence that the provider can change public-chain behaviour.

2.10 We welcome the statement at paragraph 3.41 that SYSC 15A applies to relevant third-party arrangements whether or not they amount to outsourcing. Firms remain accountable for their choice of dependencies. FG26/6 already addresses permissionless DLT use and distinguishes it from outsourcing under SYSC 8. It also discusses internal controls, monitoring, independent audits and contingency planning where direct contractual relationships are absent, and alternatives where direct testing with a third party is impossible. Building on paragraphs 4.4-4.5, 8.5-8.6 and 9.7 of FG26/6, we ask for a DeFi-specific worked example showing the evidence supervisors would accept where conventional contractual audit rights are unavailable. [16] The absence of a contract is neither an automatic prohibition nor evidence that the risks are acceptable.

2.11 Firms should test independent verification of transaction details at approval, segregation of duties, key recovery, replacement of compromised signers and continuous incident escalation. A multisignature arrangement should not be credited as independent approval merely because several people approve the same compromised screen, as case study 5 (Bybit) shows. Bug bounty programmes and coordinated vulnerability disclosure should be recognised as useful supplementary controls, with clear limits on what they establish.

**Question 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.**

## **Response**

### **Support for a functional assessment**

3.1 We agree that financial crime requires serious attention. FATF's July 2026 report calls for a functional, risk-based approach to DeFi and addresses how control is identified. [9] We support that approach, subject to the UK legislation that determines which persons and activities are in scope. FATF recommendations inform policy; they should not be presented as independently creating domestic obligations for every participant in a protocol.

3.2 We recommend distinguishing the commission of an offence, the movement of its proceeds and a customer's incidental exposure to those proceeds. Each needs different evidence. An exploit may concern contract design; laundering may involve several chains and intermediaries; an innocent recipient may receive an unsolicited transfer. A single label such as "DeFi exposure" is not enough to decide which controls are proportionate or what reporting obligation arises.

3.3 Self-custody, privacy tools, flash loans and cross-chain transfers should be treated as features requiring contextual assessment. Their presence does not establish criminal purpose, and a lawful arbitrage or refinancing transaction should not be treated as suspicious solely because it is complex. Equally, a familiar interface or well-known protocol should not displace scrutiny of the customer, the transaction and the source of funds.



The BBA CLG Ltd, Kemp House  
124 City Road  
London, EC1V 2NX, UK

3.4 Blockchain analytics should support an investigation, not decide its outcome without scrutiny. Firms should understand the evidential basis of address labels, clustering assumptions, tracing gaps and the difference between direct and remote exposure. A risk score should record its source, age and confidence. Repeated transfers through pooled liquidity should not be treated as proof that every later user knew of, owned or controlled the original proceeds.

## **Correct the sanctions description in case study 4**

3.5 Case study 4 (the \$SQUID rug pull) describes a scam launched in 2021, with the rug pull in November 2021, and states that the scammers “then used the OFAC-designated mixer Tornado Cash” to launder the proceeds. [5] That description is anachronistic. TRM Labs reported deposits into Tornado Cash on 1 November 2021. [20] The US Treasury did not designate Tornado Cash until 8 August 2022. [12] In Van Loon, the Fifth Circuit held on 26 November 2024 that Tornado Cash’s immutable smart contracts were not property capable of being blocked under the International Emergency Economic Powers Act, and that OFAC had therefore exceeded its statutory authority. [17] OFAC subsequently removed Tornado Cash from the SDN List on 21 March 2025. [13] The designation did not apply at the time of the incident and was subsequently removed.

3.6 We ask the FCA to separate the laundering conduct from the later designation and delisting, and to date both. This does not diminish the underlying money-laundering risk of mixing services, which the case study rightly illustrates. By contrast, Lazarus Group remains on OFAC’s SDN List as at 22 October 2026, so the correction should be specific to Tornado Cash. [21]

3.7 The guidance should also distinguish an OFAC designation from a prohibition under an applicable UK sanctions regime. Firms must assess the jurisdictions and legal obligations that actually apply to their activities. Historic intelligence can remain relevant to risk, but current restrictions must be checked against the relevant current legal instruments and lists. A historic vendor label should not substitute for that exercise.

3.8 More generally, we recommend adding dates, primary references and attribution limits to every case study. Case study 5 already identifies the compromised Safe Wallet interface and the deception of Bybit’s transaction approvers. That level of precision, applied across all six case studies, makes them more useful to supervisors and avoids treating evidence about one component as evidence about every DeFi business model. [5]

**Question 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?**

## **Response**

### **Customer identification and transaction evidence**

4.1 We support customer due diligence, enhanced checks where legally required, and ongoing monitoring proportionate to risk. The final guidance should explain whose identity a firm must establish in common DeFi transactions. The firm’s own customer, a beneficial owner where



The BBA CLG Ltd, Kemp House  
124 City Road  
London, EC1V 2NX, UK

relevant, a contractual counterparty and an unidentified participant in a liquidity pool are not interchangeable. We recommend worked examples that identify the legal basis for the information sought and explain what follows if it cannot be obtained.

4.2 The Travel Rule discussion should be more precise. Paragraph 4.26 refers to “Regulation 64 of the MLRs (the Travel Rule)”, but the cryptoasset Travel Rule sits in Part 7A of the MLRs. Paragraph 4.27 then notes that cryptoasset businesses may request information from their customers under regulation 64G. It omits two elements. Regulation 64G(2) and (3) require a cryptoasset business deciding whether to request information under regulation 64G(1) to have regard to its risk assessments and to assess the transfer against specified risk factors. Regulation 64G(4) provides that, if information requested under regulation 64G(1) is not received, the cryptoasset business must not make the cryptoasset available to the beneficiary. [8] The final guidance should state both, so that it neither implies a universal obligation to identify every remote wallet holder nor suggests that a cryptoasset business may disregard the statutory consequence of an unanswered request.

4.3 We recommend examples covering a customer depositing from their own wallet, withdrawing to another person’s wallet and receiving assets after interacting with a pool. The FCA should distinguish evidence of technical control of an address from evidence of identity and source of funds. A signed message may help establish control at a particular time; it cannot by itself establish identity or source of funds. Identity information should be exchanged through appropriate secure channels, not published on a permanent public ledger.

4.4 We welcome the expectation at paragraph 4.28 that firms maintain procedures for missing or incomplete information. Those procedures should also cover incomplete tracing and conflicting analytics. Relevant controls may include further enquiries, manual review, exposure limits or declining a transaction where necessary. Decisions should be recorded and capable of review. Customers should receive explanations where lawful, without compromising reporting restrictions or an investigation. Correction procedures matter most where an innocent customer is affected by a mistaken address attribution.

## **Prevention and response**

4.5 We recommend assessing each point at which a firm can intervene: onboarding, transaction preparation, signing, submission, receipt and subsequent monitoring. Screening only after an irreversible transfer may identify a problem too late to prevent it. Equally, pre-transaction simulation cannot guarantee execution against an unchanged state. Controls should account for the interval between review and execution, and for changes in contract permissions or destinations.

4.6 Paragraph 4.25 rightly asks firms to understand the difference between reporting suspicion to the NCA and sanctions requirements. We suggest adding a short routing example that also covers operational incident notifications, showing the responsible authority, trigger and information required for each, while leaving the legal thresholds intact. Firms should preserve transaction hashes, chain identifiers, relevant contract versions, timestamps and the basis for attribution. A push to improve reporting quality should not become a target for the volume of reports filed.



The BBA CLG Ltd, Kemp House  
124 City Road  
London, EC1V 2NX, UK

4.7 Privacy-preserving credentials and zero-knowledge proofs merit supervised testing. A proof can establish a specified statement under a particular system, including that a credential was not revoked at a specified time. It does not, by itself, establish the reliability of the underlying identity evidence, whether the credential remains valid after that time, or facts about source of funds beyond the statement proved. [23, 24] We propose trials covering issuance, revocation, audit access, data protection and lawful disclosure, assessed against the applicable obligations without presuming that a technical proof satisfies them.

4.8 Compliance should remain achievable for smaller firms. We recommend accepting suitable shared intelligence, independent assurance and specialist services, while requiring each firm to understand their limitations and retain responsibility. The FCA should avoid prescribing a vendor, tracing product or universal numerical risk threshold, and should instead assess whether a firm's controls work for its actual customers, services and exposures.

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

### **Response**

#### **Benefits that merit testing**

5.1 DeFi offers programmable transactions, independently inspectable records and services that operate beyond conventional trading hours. These capabilities may reduce particular processing and reconciliation burdens. The technical literature explains how smart contracts and composable protocols can provide financial functions. [11] The policy case should nevertheless be tested against total costs, including collateral, execution, security and compliance. We do not claim that DeFi is necessarily cheaper or more inclusive than the alternatives.

5.2 Eli and Alexandre propose a lending-rate discovery mechanism and evaluate it through simulations. [3] This gives a research basis for experimenting with transparent pricing; it does not establish that UK households or businesses will obtain cheaper credit. We propose controlled trials against a conventional comparator, recording realised borrowing costs, defaults, liquidity and recoveries. Where a mechanism depends on borrower information, the trial should test the quality of that information and the incentives behind it.

5.3 Governance can also be improved through deliberate design. Lustenberger, Küng and Spychiger use action design research to examine DAO-inspired methods for allocating research grants in a university community. [4] The relevance here is methodological: voting arrangements can be designed and evaluated rather than assumed to be fair. Financial applications need separate tests of conflicts, capture, accountability and emergency powers, and the university study should not be cited as validating token-holder governance in financial markets.

5.4 The FCA should support common standards for describing audits, protocol dependencies and material changes. Standards should make comparison possible rather than confer a badge of safety. Smaller firms should be able to reuse relevant evidence, subject to checking its scope, currency and independence. This would avoid every firm recreating the same technical investigation.

## Risks beyond the immediate scope

5.5 The draft rightly identifies sandwich attacks (table at 4.10). The FCA should distinguish harmful transaction-ordering practices from the wider category of maximal extractable value. We recommend evaluating execution quality through slippage, pricing, failed transactions and value lost through adverse ordering. Private routing may reduce some exposure but creates dependence on particular operators. Firms should explain the protection offered, the residual risk and how the outcome is measured, rather than promise that an execution route is immune from manipulation.

5.6 The draft discusses the opportunities and risks of agentic AI (3.9 and 4.10). Automated agents need clear spending permissions, transaction limits, revocation arrangements and an identified person responsible for the service. We propose testing malicious instructions, compromised data, rapid repeated transactions and failure of a monitoring service. The use of an agent should not change the identity of the regulated firm or obscure responsibility for customer decisions and losses.

5.7 Consumer communications should identify the service provider, material dependencies, withdrawal constraints, potential losses and any applicable complaints or compensation arrangements. Firms should explain whether a quoted yield reflects fees, borrowing demand, token incentives or another source. The availability of an interface should not imply that the underlying investment or protocol has FCA approval, and a client's acceptance of disclosed risks should not be treated as curing a failure to comply with applicable duties.

5.8 The UK should encourage experiments with supervisory access to verifiable data. Auer's work on embedded supervision provides a conceptual basis for using ledger information in oversight. [14] We recommend trials in which firms and supervisors agree data definitions and independently test completeness. Ledger visibility should complement, not replace, evidence about liabilities, off-chain assets and legal obligations. A reserve balance alone cannot establish a firm's overall solvency.

## **Question 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?**

### **Response**

#### **Measures within the FCA's remit**

6.1 The FCA should publish a reusable set of financial crime compliance examples with a clear statement of their legal status. Each should describe a business model, identify the applicable obligations, set out proportionate evidence and show why the controls are sufficient or deficient. The examples should cover both acceptable use and circumstances in which a firm should not offer a service. This would reduce repeated interpretative work while preserving supervisory judgement.

6.2 We recommend a programme of coordinated incident exercises involving regulated firms, technical specialists, analytics providers and the relevant authorities. It should test rapid preservation of evidence, verified warnings, cross-chain tracing and the lawful handling of



The BBA CLG Ltd, Kemp House  
124 City Road  
London, EC1V 2NX, UK

suspected proceeds. Published outputs should describe lessons and control improvements without exposing exploitable weaknesses or personal data. Any compulsory information-sharing arrangement would need an appropriate legal basis.

## Measures requiring wider coordination

6.3 The FCA, HM Treasury, law enforcement and the relevant sanctions authorities should clarify how the different regimes operate together. We recommend a common set of transaction examples rather than a new general category of “DeFi licence”. Where legislation is needed, the proposed duty, the responsible person and the territorial connection should be identified expressly. Guidance should not be used to extend the perimeter where that requires legislation.

6.4 Financial crime policy should focus on effective supervision and cooperation as well as formal rules. FATF’s July 2026 report identifies substantial difficulties in assessing DeFi risks, identifying qualifying arrangements and the persons exercising control, and applying licensing, supervisory and enforcement measures. [9] The UK should support compatible information standards and cross-border investigations. It should not assume that identical legal structures are needed in every jurisdiction, or that an overseas registration establishes equivalent controls. Cooperation should rest on evidence of supervision and practical assistance.

## Implementation and UK benefits

These comments fall outside the six questions but bear directly on whether the final guidance works in practice.

7.1 We ask the FCA to test the practical burden of implementation. Paragraph 1.10 of the consultation introduction (page 2) states that section 138I of FSMA does not require a cost benefit analysis for guidance. Section 139A does not import that statutory requirement. [18] The FCA’s published policy nevertheless provides for a cost benefit analysis where a high-level assessment of general guidance about rules identifies novel measures that may, in effect, prescribe or prohibit conduct and cause significant costs. [19] We ask the FCA to explain how it has applied that policy here and to test its expectation that the guidance will not materially change firms’ costs. A focused exercise should estimate cost by business model and firm size, assess the availability of qualified specialists, and examine whether the approach creates avoidable dependence on a small group of vendors. Any transitional arrangements should be explained without suggesting the suspension of obligations already in force.

7.2 The UK can benefit if firms can establish, before committing capital, what service they may lawfully offer and what evidence will satisfy the regulator. Clear requirements could support investment in engineering, assurance, legal services and financial crime expertise, and a UK market in security assurance and tokenomics analysis. These are plausible channels of benefit, not quantified forecasts. We do not assign a GDP or employment figure to DeFi because the cited research does not establish one.

7.3 Useful adoption should be measured through services delivered: processing cost, settlement failures, withdrawal reliability, consumer losses, reporting quality and entry by viable firms. Token prices and total value locked should not be used as substitutes for those outcomes. We recommend a review twelve months after the guidance takes effect, with



The BBA CLG Ltd, Kemp House  
124 City Road  
London, EC1V 2NX, UK

published findings on compliance costs, competition and harm, so that the FCA can revise its expectations against observed results.

Proposed amendments to the final guidance

The following text is proposed for consideration. It is not a quotation from the consultation or a statement of additional existing duties.

## **Scope and legal status**

Paragraph 1.4 of the consultation introduction (page 2) and paragraphs 1.9, 1.11 and 1.12 of the draft guidance (page 5) already cover much of this ground. We suggest drawing them together in a single opening statement: [5]

“Firms should first identify the statutory and Handbook provisions applicable to their activities. References in this guidance to DeFi participants, technologies or business models do not by themselves determine whether a person carries on a regulated activity. Illustrative practices are not mandatory in every case. Firms should be able to explain how the approach they adopt meets the requirements applicable to them.”

## **Dependencies outside the firm’s control**

“A firm’s inability to modify a public protocol does not remove its responsibility to comply with applicable operational resilience requirements. Its assessment should identify the measures available to it, test their effectiveness and establish whether it can deliver its important business services within the applicable impact tolerances, taking account of SYSC 15A.2.10G. Where it cannot do so, it should change or restrict the service or refrain from providing it.”

## **Financial crime indicators**

“The use of self-custody, privacy-enhancing technology or a cross-chain service does not, without consideration of the circumstances, establish illicit activity. Firms should assess relevant indicators in context, understand the limitations of analytical tools and record the basis of material decisions. This does not displace any applicable prohibition, due diligence requirement or reporting obligation.”

## **Travel Rule**

“Cryptoasset businesses must comply with Part 7A of the MLRs where it applies to a cryptoasset transfer. When deciding whether to request information from its customer under regulation 64G(1), a cryptoasset business involved in an unhosted wallet transfer must have regard to the risk assessments specified in regulation 64G(2). Its assessment of the transfer’s risk must take account of the factors specified in regulation 64G(3). If information requested under regulation 64G(1) is not received, the cryptoasset business must not make the cryptoasset available to the beneficiary, as required by regulation 64G(4).”

## **Sanctions references in case studies**

“Case studies should identify the date and jurisdiction of any designation and distinguish its status at the relevant time from subsequent changes. Historic associations may inform a risk



The BBA CLG Ltd, Kemp House  
124 City Road  
London, EC1V 2NX, UK

assessment but do not replace an assessment of the sanctions obligations currently applicable to the firm and transaction.”

## Closing position

We support demanding standards for firms that choose to provide financial services through DeFi. Those standards should identify a legally responsible person, address a demonstrable risk and allow firms to show that their chosen controls work. Regulation should also leave room to test useful services and recognise where public infrastructure improves scrutiny. We invite the FCA to adopt the amendments and implementation measures above, with the technical and evidential detail needed to make the final guidance workable.

We would be glad to discuss any part of this response.

Yours faithfully,

**The British Blockchain Association**  
Research Department  
The Centre for Evidence-Based Blockchain

---

## References

- [1] M. Hafner, R. de Luze, N. Greber, J. Beccuti, B. Biondi, G. Katten, M. Riccobene and A. Arrigoni, “DeFi Lending Platform Liquidity Risk: The Example of Folks Finance”, The Journal of The British Blockchain Association, vol. 6, no. 1, 2023. DOI: 10.31585/jbba-6-1-(5)2023. [Source](#)
- [2] S. Kampakis and L. Stankevičius, “The Tokenomics Audit Checklist: Presentation and Examples from the Audit of a DeFi project, Terra/Luna and Ethereum 2.0”, The Journal of The British Blockchain Association, vol. 6, no. 2, 2023. DOI: 10.31585/jbba-6-2-(1)2023. [Source](#)
- [3] C. Eli and H. Alexandre, “Rate Discovery in Decentralised Lending”, The Journal of The British Blockchain Association, vol. 8, no. 2, 2025. DOI: 10.31585/jbba-8-2-(7)2025. [Source](#)
- [4] M. Lustenberger, L. Küng and F. Spychiger, “Designing Community Governance – Learnings from DAOs”, The Journal of The British Blockchain Association, vol. 8, no. 1, 2025. DOI: 10.31585/jbba-8-1-(4)2025. [Source](#)
- [5] Financial Conduct Authority, GC26/7: Decentralised Finance, 21 October 2026. Consultation introduction: paragraphs 1.4 and 1.10 (p. 2); questions: p. 3. Draft guidance: paragraphs 1.9-1.16, 2.1-2.3, 3.4, 3.17-3.42 and 4.25-4.28; case studies 1-6. The introduction and draft guidance have separate paragraph numbering. [Source](#)
- [6] Financial Conduct Authority, CP26/36: Cryptoasset Perimeter Guidance, 21 October 2026. Chapter 6 and proposed PERG 18.8.25. [Source](#)
- [7] FCA Handbook, SYSC 15A.2, in particular SYSC 15A.2.5R and SYSC 15A.2.9R–15A.2.11G. [Source](#)
- [8] The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, SI 2017/692, as amended, Part 7A, regulation 64G(1)–(4). [Source](#)
- [9] Financial Action Task Force, Targeted Report on Regulatory Challenges from Decentralised Finance, July 2026, especially paragraphs 20-21 and footnote 25. [Source](#)



The BBA CLG Ltd, Kemp House  
124 City Road  
London, EC1V 2NX, UK

- [10] T. Barbereau, R. Smethurst, O. Papageorgiou, J. Sedlmeir and G. Fridgen, “Decentralised Finance’s timocratic governance: The distribution and exercise of tokenised voting rights”, *Technology in Society*, vol. 73, 102251, 2023. DOI: 10.1016/j.techsoc.2023.102251. [Source](#)
- [11] R. Auer, B. Haslhofer, S. Kitzler, P. Saggese and F. Victor, *The Technology of Decentralized Finance (DeFi)*, BIS Working Papers No. 1066, January 2023. [Source](#)
- [12] US Department of the Treasury, “U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash”, press release, 8 August 2022. [Source](#)
- [13] Office of Foreign Assets Control, *Cyber-related Designation Removal; North Korea Designation Update and Removal*, 21 March 2025 (removal of Tornado Cash from the SDN List). [Source](#)
- [14] R. Auer, *Embedded supervision: how to build regulation into decentralised finance*, BIS Working Papers No. 811, September 2019, revised May 2022. [Source](#)
- [15] Financial Conduct Authority, PS26/18: *Cryptoasset perimeter guidance*, 16 September 2026. [Source](#)
- [16] Financial Conduct Authority, FG26/6: *Guidance on Cryptoasset Operational Resilience*, 30 June 2026, especially paragraphs 4.4-4.5, 8.5-8.6 and 9.7. [Source](#)
- [17] *Van Loon v. Department of the Treasury*, No. 23-50669, US Court of Appeals for the Fifth Circuit, judgment of 26 November 2024, pp. 2 and 33-34. [Source](#)
- [18] *Financial Services and Markets Act 2000*, section 139A(5), read with section 138I. [Source](#)
- [19] Financial Conduct Authority, *Statement of Policy on Cost Benefit Analyses*, July 2024, paragraphs 3.7-3.9 (p. 9). [Source](#)
- [20] TRM Labs, *On the Trail of the Squid Game Scammers*, 11 January 2023; investigation identifying Tornado Cash deposits on 1 November 2021. [Source](#)
- [21] Office of Foreign Assets Control, *Sanctions List Search*, Lazarus Group, SDN entry 27307, programme DPRK3; checked 22 October 2026. [Source](#)
- [22] *Draft Financial Services and Markets Act 2000 (Cryptoassets) (Miscellaneous Amendments) Regulations 2026*, regulation 4(5)(b)(viii), proposed article 9Z2A; laid before Parliament on 15 September 2026. [Source](#)
- [23] AnonCreds Working Group, *AnonCreds Specification*, v1.0 Draft, sections on non-revocation proofs and revocation registries; accessed 22 October 2026. [Source](#)
- [24] World Wide Web Consortium, *Verifiable Credentials Data Model v2.0*, W3C Recommendation, 15 May 2025, section 2, definition of verification. [Source](#)