GBBC response to FCA GC26/7 on DeFi

About Global Blockchain Business Council (GBBC)

GBBC is the largest leading non-profit association for the blockchain, digital assets, and emerging technologies community. Founded in 2017 in Davos, Switzerland, GBBC comprises more than 500 institutional members and 251 Ambassadors across 119 jurisdictions and disciplines.

GBBC furthers adoption of digital technologies by engaging regulators, business leaders, and global changemakers to harness these transformative tools for more secure and functional societies.

GBBC industry verticals: Financial Services, Global Commerce/Supply Chains, and Commodities, underpinned by AI, digital identity, governance, hardware, infrastructure, policy, regulation, and security.

GBBC initiatives: BITA Standards Council (BITA), GBBC Digital Media, Global Standards Mapping Initiative (GSMI), International Journal of Blockchain Law (IJBL), InterWork Alliance (IWA), and U.S. Blockchain Coalition (USBC).

Summary of recommendations

GBBC supports the FCA's aim of helping firms manage operational and financial crime risks when using DeFi. Firms remain accountable for the services they provide, and the guidance should explain how they can demonstrate compliance where they do not control the underlying infrastructure. It should distinguish risks arising from distributed ledger technology (DLT) infrastructure from those arising from DeFi arrangements, integrate with existing operational resilience frameworks, and explain how financial crime requirements apply to representative transactions.

Our principal recommendations are:

- Distinguish DLT infrastructure risks from DeFi service risks, and explain how firms can protect the integrity and resilience of their own records without controlling the network.
- Integrate DeFi risk management with firms' existing resilience frameworks and clarify incident reporting, notifications and registers where there is no conventional service provider or contract.
- Give firms practical examples of how to test services and plan recovery where protocol cooperation is unavailable and assets cannot immediately be withdrawn.
- Explain how the Travel Rule applies to the parties and stages of representative transactions, including who can supply or receive information and when a firm can intervene.
- Apply a risk-based approach to unhosted wallets, clarify the interaction with the proposed Financial Crime Guide updates, and explain how source-of-funds and source-of-wealth assessments should work in DeFi.
- Test transaction journeys with industry and the Joint Money Laundering Steering Group (JMLSG), and refer evidenced legislative difficulties to HM Treasury where guidance cannot resolve them.

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.

We broadly agree with the FCA's description of the principal risks. The guidance should distinguish risks arising from the underlying DLT infrastructure from those associated with a DeFi service, and give greater attention to failures affecting both a service and its recovery arrangements.

This can arise where two protocols depend on the same oracle, bridge or infrastructure provider, so that a single failure disrupts both the service and its fallback. We recommend that the FCA

use practical examples to show how firms can identify these common dependencies and test whether an alternative route provides independent capacity.

The Sui outage case study illustrates a risk at the network infrastructure level. Such disruption can affect a financial institution using DLT even where its service does not involve DeFi. The final guidance should identify which risks arise at the network level and which depend on a protocol's design, governance or financial activity, so that firms can assess the relevant dependencies without treating every use of DLT as DeFi.

A firm may not control all the nodes or the network's recovery, but it can assess the resilience of its chosen infrastructure and protect the integrity and availability of the records it uses. We recommend examples covering independent validation of ledger data, reconciliation with internal records, monitoring of finality and inconsistencies, and tested procedures for pausing activity and resynchronising records after disruption. Those controls should be assessed against the service and data at risk; maintaining an independent record does not itself restore on-chain settlement or access to assets.

GBBC's Capital Markets Risk Mitigation Framework (RMF), developed with Oliver Wyman and industry participants, provides a useful reference. It distinguishes measures available to blockchain ecosystems from those available to financial institutions, including reconciliation, monitoring and failover arrangements. The FCA should draw on that distinction when explaining what firms can do within their own systems and how they should assess risks outside their control.

The assessment should also consider whether firms can continue to deliver the service to customers, including whether withdrawals can settle, collateral can be released and an alternative route has sufficient liquidity. This would build on the FCA's existing guidance on dependency and concentration risk.

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?

We agree with the direction of the proposed guidance. It should explain how firms can use their existing operational resilience arrangements to address DeFi dependencies, alongside practical examples of testing without protocol cooperation and recovery where assets cannot immediately be withdrawn.

Our response to CP25/25 Part II supported senior-manager accountability while asking the FCA to clarify the reasonable steps firms can take when relying on decentralised infrastructure. A firm cannot control a public network's consensus, but it can assess network risk and oversee the functions within its own service. The same distinction is relevant to the expectations for testing and recovery.

Consistency with existing resilience frameworks

For firms already subject to operational resilience requirements across their wider business, DeFi dependencies should be incorporated into existing service mapping, impact tolerances, testing and incident management. The FCA should explain where its proposed guidance adds detail to those arrangements and what further evidence is needed for a particular DeFi exposure. Firms should be able to use existing controls and assurance where they address the relevant risk, with additional work directed at identifiable gaps.

A short mapping annex should connect GC26/7 with SYSC 15A and the incident and third-party reporting requirements, distinguishing their respective scope and purpose. For firms also subject to the EU's Digital Operational Resilience Act (DORA) and Markets in Crypto-Assets Regulation (MiCA), the FCA should explain how relevant mapping, testing and assurance evidence may support a UK assessment, and where UK-specific evidence is needed. This would build on our MiCA review recommendation on avoiding repeated assurance, without treating compliance with another regime as sufficient for UK purposes.

Incident and third-party reporting

The final guidance should address the interaction with the FCA and PRA operational incident and material third-party reporting regimes taking effect on 18 March 2027. PS26/2 and PRA PS7/26 establish coordinated reporting arrangements, but firms using decentralised infrastructure may not have a conventional service contract or an identifiable provider able to supply the information requested. The final guidance should explain how those dependencies are assessed and reported by firms within scope.

FG26/4 defines a third-party arrangement broadly, while its templates seek provider and contractual information. The FCA should distinguish direct reliance on a public network from the use of an identifiable service provider, such as a node or access provider, and explain when each falls within the relevant definition. For arrangements in scope, examples should show how to complete the notification and register where conventional contract or provider details are unavailable, including how to record that limitation. The absence of a written contract should not, by itself, be presented as resolving the assessment.

Operational incident reporting requires a separate assessment. A network disruption may affect a firm's services or customer data even where no reportable third-party arrangement has been identified. Building on FG26/3, the FCA should show how a firm applies the reporting thresholds using the impact on its own operations, reports information available to it and updates its account as the cause becomes clearer. Examples should avoid assuming that the firm can obtain a provider's incident report or wait for network-wide attribution before assessing its own reporting obligations.

Testing without protocol cooperation

We recommend that paragraphs 3.32 and 3.39–3.41 include examples of testing a firm can undertake without a protocol operator's participation. These could cover replaying historical disruptions, testing a local copy of the software and modelling congestion, delayed finality or

failed exits. When recording the results, firms should distinguish direct testing from independent evidence and explain material assumptions, including the limitations of simulations that cannot replicate live particiant behaviour. They remain responsible for assessing whether that evidence is sufficient and for meeting their applicable obligations.

We also recommend that the FCA recognise existing independent audits where their scope and currency address the relevant risk. As GBBC argued in its MiCA review response, firms should be able to use assurance within its stated scope without unnecessarily repeating equivalent work. Relying on an audit would still require firms to check the deployed version, configuration, unresolved findings and subsequent changes, and to assess risks outside its scope. This is particularly relevant to live liquidity and recovery capacity, which a code audit cannot establish.

Recovery where assets cannot be withdrawn

Recovery planning also needs to address incidents where a firm can stop new transactions but cannot immediately withdraw existing assets. For each action, the plan should identify who can take it, what triggers it and how long it will take, covering both the steps to limit further exposure and those needed to recover existing positions.

For staking or vault services, this means testing withdrawal queues, network availability, collateral requirements and liquidity. Firms should assess whether an alternative remains available under stress, has sufficient capacity and depends on the failed component, as well as whether it is legally permissible and operationally executable. Moving assets through another bridge, for example, can introduce a different dependency that the assessment needs to consider.

The plan should draw on these assessments to record a credible recovery time and the assumptions supporting it. Where a firm cannot meet applicable requirements, it should change the service, reduce the dependency or refrain from the activity as appropriate. Accepting residual risk or disclosing it to customers does not itself discharge those requirements.

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.

We recognise the financial crime risks identified by the FCA. The final guidance should help firms assess each transaction in context and explain how familiar concepts, including source of funds and source of wealth, apply to DeFi activity.

For example, a transaction crossing a bridge may reflect a customer's access to a service, while its routing, timing or links to illicit activity may warrant further enquiry. To assess that risk, firms need to understand what an alert actually shows and how reliable the attribution is. We would welcome examples of how customer information, the purpose and value of a transaction, and the strength of an on-chain link can be assessed together, with sanctions requirements considered separately.

A contextual assessment is also relevant to unhosted wallets. In its 2022 response, HM Treasury recognised their legitimate uses and rejected treating their transactions as automatically higher risk when setting the Travel Rule approach. Neither the wallet type nor a low analytics score should determine the assessment on its own.

The treatment of unhosted wallets in CP26/38 would benefit from further explanation. Its example of good practice describes a firm applying enhanced due diligence (EDD) to transactions involving these wallets. Although a preceding example refers to applying EDD where appropriate to higher-risk activity, the unhosted-wallet example does not explain the circumstances. Firms could therefore read it as an expectation to apply EDD to every such transaction, irrespective of the wider assessment.

Given that the tests for enhanced customer due diligence and Travel Rule information requests are distinct, we recommend that the FCA explain how GC26/7 and CP26/38 interact. This should cover when self-custody is a relevant risk factor, what further evidence may justify enhanced checks and when EDD is legally required. Mandatory EDD requirements continue to apply.

Paragraph 4.15's reference to source-of-wealth and source-of-funds risks also needs practical context. Identifying the wallet or protocol from which an asset arrived may help trace a transaction without explaining how the customer acquired the funds or accumulated their wealth. The guidance should make those evidential questions explicit and connect them to the controls discussed in our answer to Question 4.

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?

We recommend that the FCA publish a practical annex to paragraphs 4.26–4.28, using representative transactions to explain the Travel Rule obligations at each stage. While the draft recognises that firms may have difficulty obtaining and transmitting information, firms still need to understand how to identify the relevant transfer, what information is required and when they can act.

The fit between the Travel Rule and DeFi transactions

We encourage the FCA to distinguish between intermediated cryptoasset activities, where identifiable persons perform relevant functions, and direct interactions with autonomous protocols, where there may be no receiving institution. Where users interact through unhosted wallets, an autonomous smart contract may have no operator responsible for collecting, verifying, transmitting or retaining beneficiary information. The conventional allocation of responsibilities between originating and receiving cryptoasset businesses may therefore be difficult to apply. The guidance should identify the duties arising from each person's activity and explain how they can be discharged where control over execution or access to counterparty

information is limited. A contract address can show where assets moved, but does not, by itself, identify a legal counterparty, establish that a receiving cryptoasset business exists or identify the beneficiary for the relevant purpose.

These questions arise alongside implementation difficulties that extend beyond DeFi. The FCA's Travel Rule statement addresses uneven international implementation, while FATF recorded industry concerns about interoperability between compliance tools in 2024. For DeFi arrangements, firms also need to understand the process that applies on the particular facts, whether a transfer has no identifiable receiving business or involves a business with no available messaging channel.

To resolve these questions, the assessment needs to start with each person's activity and the relevant statutory definitions. Proposed guidance in CP26/36 states that the exclusion for certain technical services from arranging does not extend to Regulation 14A of the Money Laundering Regulations (MLRs), so the MLR position requires a separate assessment. A DeFi label, absence of custody or missing messaging facility does not settle that assessment on its own.

DeFi transactions can involve several smart contracts, liquidity pools and lending protocols, with multiple operations executing atomically within a single transaction on one blockchain. A wider transaction journey may also involve cross-chain bridges. Where execution is atomic, there may be no opportunity for an intermediary to pause between operations to obtain or exchange information. The proposed annex should explain which movements constitute relevant transfers for Travel Rule purposes and which information must be exchanged before execution, including how this can be achieved. It should distinguish these arrangements from transfers with separate settlement stages at which a firm can intervene.

Worked transaction examples

The following illustrative examples would help firms apply the guidance. For each, the FCA should state the assumptions, identify the persons and functions involved, and explain which movements are relevant transfers and which duties apply:

1. A customer instructs an exchange to transfer assets to their own unhosted wallet, then later uses that wallet to interact with an independently chosen protocol. The exchange does not route the later transaction. The example should explain how the exchange assesses the wallet and transfer, what information it may need from its customer and what it must do before making the transfer. It should also distinguish those obligations from the customer's later activity, which does not necessarily involve a service provided by the exchange.
2. A regulated firm selects a vault or liquidity pool and routes a customer's assets to it, where the contract pools assets and may issue a receipt token. Here, the example

should examine each movement, the functions performed by the firm and any vault operator, and whether a receiving cryptoasset business can be identified. For each relevant transfer, it should explain how the originator and beneficiary are determined, what information is required and who can receive it. Neither the contract address nor the receipt token alone resolves those questions.

3. One cryptoasset business sends assets to another business using a decentralised protocol for execution or settlement. In this case, the example should explain how the sending firm identifies the receiving business, transmits any required information securely and handles missing information or incompatible messaging arrangements. The use of a protocol does not, on its own, determine the nature of the receiving wallet.
4. A customer independently uses a protocol and subsequently transfers assets to a regulated custodian. This example should distinguish the asset arriving on-chain from the custodian making it available to the customer, and explain when the custodian may need information from that customer and what happens if it remains unavailable. The earlier protocol interaction does not, by itself, establish that an intermediary was involved at that stage.

Mapping these roles and decision points would build on our CP26/13 response, which asked the FCA to assess whether a DeFi interface actually controls assets or execution. It would also reflect our MiCA review response, which supported proportionate intermediary due diligence where the intermediary selects, promotes, routes or integrates access. In applying those positions here, the firm's MLR duties would still need to be assessed separately.

Information requirements and intervention

The examples also need to distinguish between obstacles that call for different responses. The guidance should explain the applicable process where:

- information does not exist or is not available to the firm;
- information exists but cannot reliably be verified;
- there is no identifiable receiving business or suitable channel for transmitting information; or
- a stage executes automatically and the firm cannot stop or reverse it.

For each of these situations, firms need guidance that distinguishes collecting, verifying, transmitting and retaining information, identifies any recipient and explains when they must decide whether to proceed. A missing messaging endpoint does not necessarily prevent a firm from seeking information from its own customer. Equally, a visible on-chain transaction does not, by itself, establish a person's identity or satisfy an information requirement.

For transfers involving unhosted wallets, paragraph 4.27 should explain the risk assessment and the process for requesting information under Regulation 64G and JMLSG guidance. Where a firm determines that information should be requested and it is not provided, JMLSG states that the firm must not make the unhosted-wallet transfer or make the cryptoasset available to the beneficiary.

An asset can arrive on a blockchain before a custodian makes it available to a customer, so a custodian that controls release may be able to withhold access even if it cannot prevent the incoming transfer. In an automated flow, by contrast, a later stage may already have executed before an alert is reviewed. We would welcome examples showing which checks must take place before signing or execution, when release can be withheld and what escalation remains possible afterwards. Firms should establish those capabilities before integration, since later monitoring cannot replace a required pre-execution check.

Source of funds and source of wealth

We recommend worked examples alongside paragraphs 4.15 and 4.20 explaining how firms should assess source of funds and source of wealth where a customer has used DeFi. Source of funds concerns the origin of the assets involved in the activity under review; source of wealth concerns how the customer accumulated their overall wealth. The guidance should explain when further enquiries into either are appropriate or required, how the assessment relates to the customer's risk profile and what evidence can reasonably support it.

For example, where a customer withdraws assets from a lending protocol or vault, the firm may need to distinguish the customer's original contribution from returns earned or amounts borrowed. Evidence of the withdrawal alone would not explain the origin of the contribution. The FCA should show how information from the customer, records of acquisition and protocol activity, and on-chain analysis can be assessed together. The examples should also address funds that have passed through several wallets or bridges, where a visible route may leave gaps in the explanation or attribution.

The examples should distinguish evidence that establishes a transaction path from evidence supporting the customer's explanation of its economic origin. Where records are incomplete or an explanation cannot be corroborated, firms need to understand what further enquiries, escalation or restrictions the applicable requirements call for. The FCA should explain the limits of relying on a protocol label, wallet signature or analytics result, while allowing firms to assess the available evidence on its merits. This should remain distinct from the Travel Rule information duties and should not imply that every DeFi transaction requires the same enquiries.

Risk-based controls and customer information

Where an alert links a wallet through a bridge to suspected illicit activity, further enquiry may be justified. The firm should assess what the data supports, its confidence in the attribution and its relevance to the customer and transaction. Customer information and the purpose of the

activity can inform that assessment. If material uncertainty remains, it should document that uncertainty, escalate as appropriate and decide whether it can proceed under the applicable requirements. Sanctions and suspicious activity reporting must each be considered separately.

Analytics tools, wallet labels and signatures can assist that assessment, but firms need to understand their limits. A signature can provide evidence of control at a point in time without identifying every person with access or the source of all assets, while analytics cannot replace legally required identity information. Firms should understand the basis of a vendor's assessment well enough to review an alert and record the reasons for their decision.

Linking identifiable personal information to publicly accessible blockchain addresses can expose individuals' on-chain activity and increase the risk of unauthorised access, targeted cyberattacks and other misuse. These risks also arise where the information is held off-chain in datasets that connect identities with wallet addresses. The FCA should explain how firms can meet applicable information requirements while limiting unnecessary collection, disclosure and retention. Firms should use secure channels and appropriate access controls, with retention periods reflecting applicable legal requirements. The guidance should also make clear that Travel Rule compliance does not require personal information to be published on-chain.

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

We would welcome a specific example covering curated vaults and automated strategies. As discussed in GBBC's GSMI 7.0 DeFi and Vaults report, changes to strategies, governance and dependencies can affect risk even where a vault's address remains unchanged. Its strategy, permitted assets, oracle, leverage limit or administrator permissions may change, so monitoring the address alone would not identify every material change in exposure.

The example should show how a firm records the configuration and mandate it has approved, monitors the powers of the curator or administrator, and decides when a change calls for reassessment or suspension of new allocations. The assessment should account for how quickly a change can take effect and whether the firm can detect and respond to it in time.

Where an automated agent acts for the firm, the same example should cover its permitted actions, exposure limits and revocation powers, recognising that revocation may stop future actions without unwinding completed transactions.

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?

We recommend that the FCA convene JMLSG, firms and technical specialists to work through a small number of real, anonymised transaction journeys. This would build on GBBC's call in CP25/25 Part II for crypto-specific typologies developed with financial crime partners.

For each journey, the exercise should identify the relevant duty and actor, available information, decision point, feasible controls and circumstances preventing execution or release. It should then test whether firms reach consistent decisions on the same facts, including where wallet attribution is uncertain, execution has several stages or funds originate from DeFi activity. Recording whether each problem concerns legal interpretation, unavailable information, a technical constraint or the legislation itself would help identify how it needs to be addressed.

We recommend that the FCA publish the resulting worked examples and keep them under review. It could also develop and update typologies with law enforcement and industry through existing public–private partnerships, including JMLIT+. Examples of bridge misuse or compromised wallets would help firms distinguish a risk indicator from evidence of illicit activity. In reviewing their effectiveness, the FCA should consider attribution quality, the resolution of ambiguous cases and the detection of suspicious activity, since message completion rates alone would not demonstrate effective controls.

Interpretative and technical questions should be addressed within the existing law. If the exercise demonstrates that a specific statutory requirement cannot be fulfilled in a particular arrangement, we recommend that the FCA document the problem, discuss it with HM Treasury and consider whether legislative work is needed. Alternative controls cannot waive a statutory duty.

Although GC26/7 clarifies existing requirements, it may affect the evidence firms seek, their controls and the services they offer. Before finalising the guidance, the FCA should test its expectations against representative journeys, including where firms have limited control over infrastructure, to address uncertainty that could restrict services without improving financial crime outcomes.