aave labs

18 November 2026

Financial Conduct Authority
12 Endeavour Square
London E20 1JN
By email: cp26-36@fca.org.uk; GC26-7@fca.org.uk

Re: Response to CP26/36 (Cryptoasset Perimeter Guidance) and GC26/7 (Decentralised Finance)

Dear Sir or Madam,

1. Introduction

Aave Labs welcomes the opportunity to respond to CP26/36 and GC26/7. The two papers address the same subject from different directions: when activity involving decentralised finance (DeFi) falls within the regulatory perimeter, and how regulated firms should manage the risks of interacting with DeFi. We therefore respond to both in a single letter. Part A responds to CP26/36 and Part B to GC26/7.

Aave Labs is a London-based software development company and a core contributor to the Aave Protocol, the largest decentralised lending protocol globally by total value locked.

We are grateful for the FCA's engagement with industry, including the recent roundtable on CP26/36 and GC26/7 and our meetings with FCA staff earlier this month. We welcome HM Treasury's introduction of the technical services exclusion in article 9Z2A of the Regulated Activities Order (RAO), and the FCA's recognition in PERG 18.8.25 that the exclusion is consistent with the purpose, expressed in HM Treasury's Explanatory Memorandum, of "removing unnecessary regulatory barriers while maintaining regulation of activities presenting material risks to consumers or market integrity".

We also welcome the FCA's response to points raised in our June 2026 response to the PERG consultation. In particular, CP26/36 confirms that the exclusion does not require that a provider offer no "added value or additional feature" (PERG 18.8.26); that a service may be technical even though it is designed for cryptoasset transactions, provided commercially and remunerated (PERG 18.8.27); and that remuneration must be assessed by reference to the functions for which it is paid (PERG 18.8.31). We support these paragraphs and ask that they be retained in the final guidance.

2. Summary: the features that make DeFi safer should not bring it within the perimeter

CP26/36 and GC26/7 should send the same message: the features that make DeFi safer should not be the features that bring it within the perimeter. Today the drafts pull in opposite directions. GC26/7 rightly asks regulated firms to rely on protocols that are maintained, monitored and risk-managed, and to screen out illicit activity. CP26/36 treats maintenance, risk management and screening as indicators of centralisation or discretion (PERG 18.8.30 and 18.8.32). Left unresolved, this tension would penalise the safest DeFi infrastructure and interfaces, and push UK users towards offshore services that offer fewer protections.

Our response is organised around three principles that apply across both consultations. Parts A and B set out our detailed responses to the questions in each paper.

(a) **Regulate the person that carries on the regulated activity.** The perimeter should capture persons that carry on regulated activities in relation to users' transactions, not those that build, maintain, govern or protect a protocol.

(b) **Safety is not intermediation.** Blocking scam assets, providing information such as network fees and prices, sanctions screening, and bounded risk management functions designed to protect protocols and their users during security incidents are protections, not discretion or control. These activities should not, in themselves, be treated as regulated intermediation merely because they involve technical controls or predetermined restrictions.

(c) **Keep UK users onshore.** The financial promotions and money laundering regimes, the treatment of stablecoins, the ability of regulated firms to give customers access to DeFi, and the timing of the authorisation process should not push UK users towards offshore services that offer fewer protections.

Our principal concern is the reading of article 9Z2A(2)(b) in PERG 18.8.32. That limb matters. HM Treasury included it deliberately, with real protocols in mind, and we think the guidance should give it practical effect. As drafted the guidance would treat access to a decentralised protocol as access to the services of a third person, and so subject to the authorisation condition in article 9Z2A(2)(a), whenever a person is sufficiently involved with the protocol. Because persons are almost always involved in developing, maintaining or governing a protocol, and because no authorised person stands behind a decentralised protocol, this reading would leave article 9Z2A(2)(b) with little practical application. We propose a dividing line between the two limbs based on whether any person carries on a regulated activity in relation to the user's transaction.

We also have a distinct concern with PERG 18.8.27: the draft does not give firms a workable positive understanding of what constitutes a technical service. The exclusion should be explained by reference to the functions that cryptoasset interfaces perform in practice to enable users to access and interact with underlying services and protocols, rather than by reference to an abstract notion of technicality. In both cases, the guidance describes the uncertainty rather than resolving it. That matters most to developers, technical interface providers and other protocol

participants that conclude they are outside the perimeter, because they will look to PERG, rather than pre-application engagement, to test that conclusion.

In summary, we ask the FCA to:

(a) **Technical services (PERG 18.8.27):** provide a positive, functional explanation of technical services, confirming that informational, presentational, connectivity, transaction-preparation and transaction-processing functionality through which a user accesses and interacts with an underlying service or decentralised protocol is capable of being technical, whatever its sophistication and although it is commercially provided or involves multiple steps (section 4).

(b) **Consumer protection features (PERG 18.8.30 and 18.8.31):** confirm that providing information, such as estimated network fees, and applying objective, rules-based safety measures, including preventing interaction with scam assets, are not the exercise of discretion.

(c) **Interposition (PERG 18.8.32):** confirm that the involvement of a person in developing, maintaining, governing or supporting a decentralised protocol does not, without more, mean that the technical service provider gives access to that person's services rather than to the protocol. The relevant question should be whether, viewed substantively, the user is accessing a service provided or operated by that person, including because the person exercises control over the execution or material terms of the user's transaction, rather than merely accessing protocol functionality implemented through non-discretionary code(section 4).

(d) **Decentralised protocol indicators (PERG 18.8.32):** ensure that ordinary maintenance, security upgrades, governance-directed fees and accurate description of a protocol do not of themselves count against decentralisation.

(e) **Risk management functions:** confirm that bounded, transparent, governance-mandated risk functions, such as independent risk stewards and guardians, do not defeat decentralised status and do not make the persons performing them interposed persons, including when responding to incidents affecting a protocol.

(f) **Financial promotions and money laundering (PERG 18.8.34 and 18.8.35):** work with HM Treasury so that the financial promotions and MLR regimes do not reverse the policy of article 9Z2A, and establish mutual recognition of payment stablecoins issued under comparable regimes, such as the US GENIUS Act, so that they are not subject to the financial promotion restrictions that apply to cryptoassets.

(g) **DeFi guidance (GC26/7):** recognise protocol-level risk management, published risk and listing frameworks and public permissionless blockchains as sources of resilience; use its existing powers to provide a proportionate route for authorised firms to give customers access to decentralised protocols, which the legislation does not prevent; and ensure consistency between the DeFi guidance, the perimeter guidance and intermediary rules.

(h) **Timing:** build the forbearance announced in CP26/36 into the final guidance, with clear criteria and a process allowing applicants materially affected by uncertainty concerning the technical services exclusion to update the relevant aspects of their applications once the guidance is finalised; and address the position of technical service providers where the authorisation of the firm to which they provide access remains pending when the new regime commences.

.

Part A: CP26/36

3. General perimeter (Questions 1 to 3)

Question 1. We support the approach in PS26/18 and CP26/36, which asks whether there is a person, whether that person carries on a regulated activity, and whether it does so by way of business in the UK. We agree that labels such as "DeFi" do not determine the analysis and that decentralisation exists on a spectrum (PERG 18.1.20). The corollary, which we ask the FCA to state expressly, is that where no person carries on a regulated activity by way of business, the activity is outside the perimeter even though users obtain financial outcomes from it. CP26/36 recognises this possibility (PERG 18.1.20), and stating it plainly would assist firms.

Automation and attribution (PERG 18.1.11 to 18.1.20). We agree that automation does not by itself take an activity outside the perimeter. We welcome the statements in PERG 18.1.18 that the fact that a person developed software or performed a technical function "does not, in itself, mean that the person is carrying on the particular regulated activity", and in PERG 18.1.20 that "Developing software is not, as such, a regulated activity". We ask the FCA to carry this principle through to the decentralised protocol limb of the technical services exclusion: developing, publishing or maintaining a protocol's code should not, of itself, count against the protocol being a decentralised protocol for the purposes of article 9Z2A(2)(b) (see section 4). The assessment should consider the functions actually performed by the relevant person, including whether that person retains ongoing discretion over the outcome of specific user transactions. Setting general, publicly disclosed parameters that apply automatically and uniformly to all users should not, without more, be treated as the exercise of discretion over an individual user's transaction. The relevant distinction is between establishing general protocol parameters through transparent governance and making a person-specific decision about whether, when or on what terms a particular transaction should proceed.

Question 2 (by way of business). We ask the FCA to confirm in PERG 18.2 that the by-way-of-business test applies person by person; that participants contributing to shared infrastructure are not to be treated as a single collective business; and that operating or controlling a protocol, or designing software, is not itself a regulated activity. The guidance should include examples covering token-holder governance, open-source development and independent risk management.

Question 3 (in the UK). We repeat our request that the guidance confirms that a developer does not carry on an activity in the UK solely because UK users interact directly with onchain code that it has published.

4. Technical services exclusion (Question 14)

PERG 18.8.27 and 18.8.32 deal with the two questions on which the technical services exclusion ultimately turns: what makes a service technical, and what makes a protocol decentralised. Both have the same difficulty. In each case, the draft identifies a range of factors, some more relevant than others, and then leaves their significance to the facts. The guidance effectively says that the assessment depends on the facts, that the listed factors may be relevant depending on the facts, and that their significance also depends on the facts. That is circular, and it leaves market participants unable to determine their position with any confidence.

We recognise that this is a novel area and that the FCA cannot anticipate every arrangement. We also understand what the FCA is guarding against: arrangements that call themselves decentralised but are, in substance, run by someone. We share that aim. We accept that the assessment is fact-specific, and we are not asking for a deterministic test or a checklist. But the fact that an assessment is fact-specific is not a reason to leave its basis unexplained. PERG exists so that firms and individuals can work out how the perimeter applies to them. To do that, they need to know which features of an arrangement matter, why they matter, and how they connect to the conditions in article 9Z2A. Without that, the guidance cannot do the job it is there to do.

This matters most to those who conclude that they are outside the perimeter. CP26/36 states that its objective is to help market participants determine whether they are within the perimeter and avoid inadvertent breaches, while recognising that PERG is general guidance rather than an assessment of individual business models (paragraphs 1.8 to 1.11 and Annex 1). For a firm that expects to be authorised, uncertainty can be explored through pre-application engagement and the authorisation process. A developer, technical interface provider or other protocol participant that concludes, consistently with the policy of the exclusion, that it carries on no regulated activity will not approach the FCA as an applicant. For it, the question is whether to apply at all, not which permission to seek, and PERG may be the principal means of testing that conclusion. It cannot be expected to enter an authorisation or supervisory process to establish whether it needs to do so.

Article 9Z2A(1) excludes from article 9Y arrangements under which a person (A), who is not an authorised person or a payment service provider, is "merely providing a technical service that allows another person" (C) "to access services provided by a third person or a decentralised protocol" (V). Article 9Z2A(2) then requires that V is either carrying on the relevant regulated activity as an authorised or exempt person, or is a decentralised protocol. The guidance therefore needs to answer three questions, which we address in the order in which they arise under the article and in

PERG 18.8: whether A's service is a technical service that allows C to access V (PERG 18.8.26 and 18.8.27); whether A is merely providing that service (PERG 18.8.30 and 18.8.31); and whether V is an authorised or exempt third person or a decentralised protocol (PERG 18.8.32).

A technical service that allows access (PERG 18.8.26 and 18.8.27)
As noted in section 1, we support the clarifications in PERG 18.8.26 and 18.8.27. However, the proposed guidance does not explain what makes a service technical in the first place. It states that the characterisation depends on what a service does, rather than the technology used, but does not identify the characteristics that distinguish a technical service from other services. It lists possible functionality and then says the service must remain technical only. This is circular: it restates the label without giving firms a meaningful basis for determining what falls within it.

The guidance should articulate the functional distinction firms should apply: technical access may comprise the means by which a user obtains information from, connects to and interacts with an underlying service or decentralised protocol. It is not necessarily confined to establishing a connection or passing on an unmodified instruction.

In the context of blockchain infrastructure, an interface may retrieve information from a blockchain or smart contract; organise and present wallet balances, transaction history, protocol state, rates or available liquidity in a usable form; translate a user's selections into the data and instructions required to interact with a smart contract; validate or format those instructions; estimate network requirements; and transmit or broadcast instructions to the relevant protocol. These functions may involve multiple steps and considerable technical sophistication. They are nevertheless capable of constituting technical functionality through which a user accesses and interacts with the underlying system.

The fact that an interface performs these functions does not, without more, mean that its provider is providing the underlying service or arranging the user's transaction. The functions may simply make information and functionality exposed by the underlying system accessible and usable by the user. The relevant assessment must, of course, still consider the service and arrangements as a whole and whether the provider satisfies the requirement that it merely provides the technical service. But the number, complexity or sophistication of the technical steps performed should not itself determine whether the service is technical.

The legislative context supports an interpretation grounded in the practical operation of cryptoasset interfaces. HM Treasury's Explanatory Memorandum states that the exclusion is intended to ensure that "tech interface providers are not treated as arranging transactions", while preserving the perimeter where a provider exercises discretion or is substantively involved in the transactions (paragraphs 5.9 and 6.10). It also records that the Government engaged with industry to test the draft amendments' practical operation and identify unintended consequences (paragraph 7.2). The exclusion should therefore be understood by reference to the functions through which cryptoasset interfaces actually enable users to access and

interact with services and protocols.

It would be difficult to reconcile that purpose with treating ordinary technical operations needed to make access usable as outside the exclusion merely because they go beyond a bare connection or passive transmission. We do not suggest that every interface function is technical or that substantive intermediation is excluded. The clarifications sought below give practical content to the category Treasury intended to protect, without enlarging the statutory exclusion.

We therefore ask the FCA to revise PERG 18.8.27 to provide a positive, functional explanation of technical services. The guidance should make clear that technical access may include informational, presentational, connectivity, transaction-preparation and transaction-processing functionality through which a user accesses and interacts with an underlying service or decentralised protocol. It should also clarify that such functionality is capable of remaining technical notwithstanding that it is sophisticated, commercially provided or involves multiple automated or manual steps; whether the provider has gone beyond merely providing that technical service remains a separate, fact-specific assessment under the statutory conditions.

Proposed drafting. We suggest the following amendments to the answer in PERG 18.8.27. Additions are shown underlined and deletions are shown struck through.

> 'Technical service' is not defined in the legislation. ~~The characterisation of a service as technical depends on what it does in practice, not on the technology used or the terminology used to describe it. A service does not cease to be technical because it is designed specifically for cryptoasset transactions, operates commercially, charges a fee or provides a convenient means of access. Equally, a service is not a technical service for the purposes of article 9Z2A merely because it is delivered through software.~~ For the purposes of article 9Z2A, the assessment should focus on the function performed by A in enabling C to access the relevant services or decentralised protocol. A service is not a technical service merely because it uses software or other technology; nor does it cease to be technical because it is designed for cryptoasset transactions, is commercially operated, charges a fee or provides a convenient or sophisticated means of access.
>
> ~~In the FCA's view, the expression is capable of including the provision of technological functionality, software, an interface, infrastructure, connectivity or an access mechanism through which C can access the relevant services or decentralised protocol, provided that the service remains a technical service only.~~ A technical service may comprise the technical means by which C obtains information from, connects to, or interacts with the relevant services or decentralised protocol. It may include functionality that makes the underlying system or its operation accessible and usable by C, including retrieving, processing, organising and presenting information concerning that system, and translating, formatting, validating and transmitting instructions through which C interacts with it.

~~The concept of 'technology' or 'technicality' should not be understood as meaning that anything to do with cryptoassets or blockchains will necessarily amount to a technical service, even though both cryptoassets and blockchains always involve some element of technology. It is also possible a service could be a 'technical' service without it involving any technology: it is the quality of the service that makes it technical or otherwise. In practice, however, any service in scope of this exclusion is likely to involve technology, but not all such services will be only technical services.~~ Examples may include: (1) retrieving information from a blockchain, smart contract or third-party service, including wallet balances, transaction history, protocol state, rates and available liquidity; (2) organising, translating or presenting that information in a form usable by C; (3) providing connectivity or an interface through which C can interact with the relevant service or protocol; (4) calculating or displaying technical information relevant to an interaction, such as estimated network fees; (5) converting choices or parameters specified by C into the data or instructions required to interact with a smart contract, including constructing, encoding or validating those instructions; and (6) transmitting or broadcasting instructions initiated or otherwise authorised by C, including instructions given in advance or by reference to parameters specified by C, to the relevant service or protocol.

~~The service must also satisfy the requirement that it is 'merely' provided. A technological service that incorporates functions amounting to substantive intermediation will not fall within the exclusion simply because those functions are performed by software or automated processes.~~ These functions may involve multiple steps and may be technically sophisticated. They do not, of themselves, amount to substantive intermediation merely because A performs more than a passive transmission function or because the functions are performed automatically. The relevant distinction is between providing the technical means by which C accesses and interacts with the underlying service or protocol, and independently selecting, recommending, directing or otherwise determining material aspects of C's transaction. The former may remain a technical service; the latter may indicate that A is performing a substantive intermediary function. The assessment remains fact-specific and must take account of the service and arrangements as a whole.

Merely providing a technical service: consumer protection features (PERG 18.8.30 and 18.8.31)

PERG 18.8.30 lists among the indicators of discretion whether A "recommends, ranks, filters or presents options in a manner reflecting a qualitative assessment of their suitability or merits" and whether A "decides that a proposed transaction should not proceed". The first is helpfully limited to qualitative assessments, but the second is not, so blocking a known scam asset could be read as discretion. PERG 18.8.31 gives "limiting access for technical security or legal compliance reasons" as an example of a restriction that "will not necessarily amount to substantive intermediation", but does not mention consumer protection. A self-custodial interface does not act on the user's behalf. Its role is to inform users and help them manage their own assets in

a better-informed way. Interacting directly with a blockchain is highly technical: without an interface, users would have to read raw transaction data, contract code and long hexadecimal addresses, and work out network fees themselves. An interface translates that information into a form users can understand, so that they can make sense of what they are doing and decide for themselves. High-quality self-custodial interfaces therefore routinely provide features that protect users, including:

- risk warnings;
- sanctions screening;
- preventing interaction with addresses, assets and contracts identified, on objective criteria, as associated with scams, exploits or illicit activity;
- clear signing, which shows in human-readable form what a user is about to authorise;
- estimated network (gas) fees;
- price and balance information; and
- approved withdrawal addresses.

These features inform the user or apply predetermined, objective rules uniformly to all users. They help users make their own decisions with better information, while the decision to transact, and control of the assets, remain with the user. They do not involve commercial judgement about the merits of a transaction, and they do not steer users towards one provider or protocol over another. Preventing a user from interacting with a known scam asset protects the user in the same way as sanctions screening: it is not a judgement about whether a legitimate transaction is a good one. Many of these features are the financial crime controls that GC26/7 encourages. This is consistent with where HM Treasury intended the line to fall: activities remain within scope where a service provider "exercises discretion over or is substantively involved in the transactions" (Explanatory Memorandum, paragraph 6.10). Informing users and applying objective safeguards uniformly to all users is neither. We ask the FCA to:

(a) amend PERG 18.8.31 to refer to restrictions imposed for "security, legal compliance or consumer protection reasons", and to confirm that preventing interaction with scam or malicious assets is such a restriction; and
(b) clarify in PERG 18.8.30 that providing information (such as estimated network fees, prices and balances) and warnings, and applying objective, rules-based screening uniformly to all users, including preventing interaction with scam assets, is not the exercise of discretion and does not take a provider outside the exclusion.

Proposed drafting. We suggest the following amendments to PERG 18.8.26, 18.8.30 and 18.8.31. Additions are shown underlined and deletions are shown struck through.

PERG 18.8.26: replacing the paragraph beginning "Conversely"

> Conversely, the exclusion is less likely to apply where ~~A's service is part of the process by which transactions are selected, shaped, directed, negotiated, routed or brought about. Accordingly, it is less likely to apply where A's service is not limited to facilitating another person (C) being able to interact with an authorised or exempt person or decentralised protocol through an interface,~~

~~for example, and/or where additional functionality beyond merely facilitating access is provided. This may remain the case even though instructions are submitted through an automated interface and some or all of A's functions are performed automatically.~~ A performs a substantive intermediary function in the process by which a transaction is selected, shaped, directed, negotiated, routed or brought about. The provision of additional functionality does not, without more, take a service outside the exclusion. The relevant question is whether that functionality enables C to access and interact with the relevant service or decentralised protocol, or instead involves A assuming an independent role in determining or materially influencing the user's transaction. This assessment must be made by reference to the service and arrangements as a whole, including the functions performed by A and the extent to which A acts on instructions initiated or otherwise authorised by C, including instructions given in advance or by reference to parameters specified by C.

PERG 18.8.30: adding a new final paragraph

For this purpose, the technical handling of an instruction should be distinguished from the exercise of judgement over the transaction to which it relates. Retrieving or presenting information, translating C's selections into transaction data, constructing or formatting an instruction, checking its technical validity, estimating network requirements, or transmitting an instruction initiated or otherwise authorised by C (including an instruction given in advance or by reference to parameters specified by C) does not, without more, indicate that A has exercised discretion. Nor does the application of objective, predetermined technical rules necessarily involve qualitative judgement by A. The relevant question is whether A is implementing C's instructions or specified parameters, or instead independently selects or determines material aspects of the transaction. This distinction is relevant but not conclusive: the absence of discretion does not, by itself, establish that a service is a technical service, and the assessment should also consider whether, viewed in the context of the arrangements as a whole, A performs a substantive intermediary function rather than providing the technical means through which C accesses and interacts with the relevant service or protocol.

PERG 18.8.31: amending item (3)

(3) receives, combines, modifies or routes orders as part of the transaction process~~;~~ in a manner that structures or materially affects the transaction, or involves A exercising an independent role in determining how the transaction is brought about. This should be distinguished from the technical handling of C's instructions, including their formatting, validation and transmission, where these functions do not themselves involve A assuming a substantive intermediary role in the transaction;

A third person or a decentralised protocol (article 9Z2A(2) and PERG 18.8.32)

In considering which limb of article 9Z2A(2) applies, we find it helpful to begin with what HM Treasury set out to achieve. The article offers technical service providers

two routes to the exclusion: access to a regulated firm, and access to a decentralised protocol. The Explanatory Memorandum presents the second as a route in its own right (paragraph 5.9), and explains that the Government tested the practical operation of the amendments with industry before making them (paragraph 7.2). The decentralised protocol limb was therefore written with real protocols in mind, as they are actually built, maintained and governed, rather than an idealised version that exists only in theory. Seen in that light, the question for this part of the guidance is a simple one: what is the user actually accessing?

Article 9Z2A operates on the status of the technical service provider (A). Its purpose is to prevent a person that merely provides technical access from being treated as arranging. It confers no exemption on the person or protocol to which access is given (V), or on anyone else. A person that carries on a regulated activity by way of business in the UK requires authorisation in its own right, whatever the status of any interface through which users reach it.

This answers any concern that reading article 9Z2A(2)(b) to include protocols with which persons are associated would allow an unauthorised person to sit between A and the protocol in breach of the general prohibition. It would not. If the associated person carries on a regulated activity, the general prohibition applies to that person directly, and article 9Z2A(2)(a) is the relevant condition for A. If the associated person carries on no regulated activity in relation to the transaction, there is no breach of the general prohibition to guard against, and nothing in the policy of the legislation requires A to be treated as arranging.

Article 9Z2A(2)(a) and (b) draw a distinction between access to services provided by a third person carrying on the relevant regulated activity as an authorised or exempt person, and access to a decentralised protocol. We agree with the FCA that the latter limb does not require the protocol itself to provide a service, carry on a regulated activity or be a person capable of authorisation or exemption (PERG 18.8.32). That is the right starting point. A protocol is technology that runs according to its code; it is not a person or a service provider. It must therefore be capable of practical application where users access and interact with the protocol itself, rather than a service provided by an intermediary, notwithstanding that identifiable persons may participate in its development, maintenance, governance or support. The existence of such participants cannot, without more, answer whether the object of access is a third person's service or the protocol itself.

That distinction is consistent with the policy reflected in HM Treasury's Explanatory Memorandum: technical interface providers should not be treated as arranging merely because they enable users to access services or decentralised protocols (paragraphs 5.9 and 6.10). It would risk undermining that purpose if access to a protocol could be characterised as access to a participant's service merely because persons contribute to the protocol's development or support. The relevant question remains whether a person is providing or operating the underlying service to which the user is given access, not simply whether persons participate in the protocol ecosystem.

We therefore propose the following dividing line between the two limbs:
(a) Where a person carries on a regulated activity in relation to the transaction to which A gives access (for example, by dealing as principal, or by receiving and transmitting orders as agent), A gives access to that person's services and article 9Z2A(2)(a) applies.
(b) Where no person carries on a regulated activity in relation to the transaction, because the transaction is executed by non-discretionary protocol code, A gives access to a decentralised protocol and article 9Z2A(2)(b) applies. This remains the case although persons develop, maintain, govern or manage risk for the protocol.

This reading gives each limb distinct work and makes neither redundant. Article 9Z2A(2)(a) governs access to regulated services; article 9Z2A(2)(b) governs access to protocols where no one carries on the regulated activity. By contrast, a reading under which any sufficiently involved person is "interposed" would make article 9Z2A(2)(b) unavailable for almost any protocol since persons are almost always involved with protocols in some way. Parliament is unlikely to have intended to create a limb that is incapable of practical application.

The text of article 9Z2A supports this reading. Paragraph (1) defines V by reference to what C is given access to: "services provided by a third person or a decentralised protocol". Paragraph (2)(a) is concerned with a third person only where it "is carrying on a regulated activity in relation to the services" to which C is given access. Paragraph (2)(b) asks only whether V "is a decentralised protocol"; it does not require the protocol to be a person, to provide a service or to carry on a regulated activity. HM Treasury's Explanatory Memorandum describes the exclusion in the same terms, as covering access to services "provided by one or more authorised or exempt persons or decentralised protocols" (paragraph 6.10). The involvement of identifiable persons in developing, maintaining or governing a protocol cannot therefore, of itself, turn access to the protocol into access to a third person's services. The question is whether any person carries on a regulated activity in relation to the services that C accesses.

Proposed drafting. We suggest replacing the sentence in PERG 18.8.32 stating that access to a third person's services involving a decentralised protocol does not fall within article 9Z2A(2)(b) with the following:

> "A person (P) should be regarded as interposed between A and a decentralised protocol, such that A gives access to services provided by P rather than to the protocol itself, only where P substantively provides or operates the service accessed by C. Relevant indicators may include P taking custody or control of C's cryptoassets, receiving or transmitting C's orders, selecting the counterparty or venue, determining material transaction terms, or exercising discretion over whether, when or how C's transaction is executed. Whether P is carrying on a regulated activity in relation to the transaction will ordinarily be a strong indicator, but the underlying question is what service or functionality C is accessing and by whom it is substantively provided.
>
> This may be the case, for example, where P takes custody of or exercises control over C's cryptoassets, receives and transmits C's orders, determines

> the counterparty, venue or material terms of C's transaction, or otherwise exercises discretion over whether, when or how C's transaction is executed. The involvement of persons in developing, maintaining, upgrading or governing a decentralised protocol, or in managing its risk parameters within limits set by its governance, does not of itself mean that A gives access to the services of a third person."

If the FCA retains the concept of a person being "sufficiently interposed", we ask that the concept be defined in the guidance by reference to these functional criteria so that firms can apply it with certainty.

Indicators of a decentralised protocol

The meaning of "decentralised protocol". Neither the Cryptoassets Amendment Regulations nor CP26/36 defines a "decentralised protocol". PERG 18.8.32 states that the term is context-dependent and must be read in its statutory context, and then lists factors that do not, by themselves, establish that an arrangement is a decentralised protocol. The guidance therefore tells firms what is not sufficient, but not what is. Put simply, the term describes how the protocol itself operates: whether it runs according to its code without any person controlling or operating it in a way that makes the user, in substance, that person's customer. It is a characteristic of the protocol, not an open-ended set of facts about the people around it. Because article 9Z2A(2)(b) is the route by which an interface can give access to DeFi without any person behind the protocol being authorised, this uncertainty goes to whether the exclusion can be relied on at all. Firms designing products, and FCA staff assessing applications, need a test that can be applied with reasonable certainty. We ask the FCA to set out positive indicators of a decentralised protocol alongside its existing negative indicators, framed by reference to function rather than labels. In our view, an arrangement should be treated as a decentralised protocol where:

(i) it executes transactions in accordance with publicly verifiable code, without any person having discretion over the outcome of individual users' transactions;

(ii) no identifiable person has unilateral custody or control of users' cryptoassets, or the ability to transfer, seize or redirect those assets outside the operation of the protocol's publicly disclosed code and parameters; and

(iii) changes to its code or parameters are made through transparent governance processes, subject to timelocks or equivalent controls, and any emergency powers are narrowly defined and bounded by that governance.

These should be treated as relevant positive indicators rather than cumulative conditions. A protocol should not cease to be decentralised solely because its code permits liquidations, collateral enforcement, parameter changes or narrowly bounded emergency measures, where those functions operate pursuant to publicly disclosed rules and no person has open-ended discretion over individual users' transactions or assets.

In assessing governance, our view is that the guidance should distinguish between

the existence of a governance mechanism and control by an identifiable person. Relevant considerations should include whether voting power is sufficiently distributed; whether proposals and votes are public; whether changes are subject to notice periods, timelocks or independent execution controls; whether any participant can implement changes unilaterally; and whether delegated powers are confined by objectively defined limits. The fact that governance can change protocol parameters should not itself establish that the protocol is operated by a person.

PERG 18.8.32 accepts that the involvement of persons in developing, maintaining or governing an arrangement does not necessarily prevent it from being a decentralised protocol. It then lists ongoing maintenance and adaptation, remuneration tied to protocol use, and holding out as factors pointing the other way. We can see why the FCA has looked at these, but they are really about the people around a protocol rather than the protocol itself. They are the kind of factors used to work out whether there is a person who should be regulated, as in PERG 18.1.17, and they can be present without anyone controlling or operating the protocol. Many protocols with an active developer community will show at least one of them. They should therefore matter only where they show that someone does control or operate the protocol, so that what the user accesses is, in substance, that person's service. We ask the FCA to clarify each factor as follows:

(a) **Maintenance.** Ongoing maintenance, security upgrades and adaptation are features of responsible protocol stewardship. GC26/7 rightly expects regulated firms to depend on infrastructure that is maintained, tested and upgraded. It would be inconsistent for the perimeter guidance to treat the same conduct as evidence of centralisation. The FCA itself recognises in PERG 18.1.17 that features of decentralised arrangements, including whether anyone has control over design and maintenance, may be "less relevant to determining whether there is a person who ought to be authorised for arranging deals in qualifying cryptoassets". It is difficult to see why maintenance should then carry weight in the exclusion from that same activity. Maintenance should be relevant only where it gives a person discretion over the outcome of user transactions or control over user assets.

(b) **Remuneration.** Fees set by token-holder governance and paid to a protocol's community treasury are different in kind from remuneration paid to an operator for intermediation services. We ask the guidance to say so.

(c) **Holding out.** Describing a protocol accurately, publishing documentation or providing information about how it works should not be treated as holding out a service.

(d) **The central question.** The relevant question should be whether any identifiable person has custody of user assets or discretionary control over the outcome of user transactions. Where neither is present, the arrangement should be capable of being a decentralised protocol.

Risk management functions
The same reasoning applies to the functions that help keep protocols safe. The

analysis should accommodate independent risk management. Mature protocols use independent risk managers and risk stewards that recommend or implement parameter changes within limits set by governance, and guardian functions with narrowly defined emergency powers, exercisable to protect users during incidents affecting a protocol. In the Aave Protocol, for example, these functions exercise only bounded authorities delegated by Aave DAO tokenholders. They are transparent and onchain, and subject to timelocks or other controls. They protect users; they do not give any person custody of user assets or discretion over individual transactions. We ask the FCA to confirm that such functions:

(a) do not by themselves prevent a protocol from being a decentralised protocol;
(b) do not make the persons performing them interposed persons for the purposes of article 9Z2A; and
(c) are not of themselves regulated activities.

The analysis should distinguish between bounded "implementation authority" and open-ended "managerial discretion". Relevant safeguards include an exhaustive statement of the actions available to the delegate; quantitative limits on parameter changes; restrictions preventing the delegate from increasing risk; public disclosure of actions; separation between recommendation, approval and execution; timelocks except where a defined emergency condition applies; and governance's ability to revoke the delegation. A person exercising authority within those constraints should not be treated in the same way as a person that can determine transaction outcomes or operate the protocol for its own account.

Treating user-protective risk controls as evidence of control would create an incentive to remove them, contrary to the operational resilience outcomes that GC26/7 seeks.

Protocol infrastructure providers

CP26/36 does not explain how article 9Z2A applies to persons supplying protocol-level infrastructure, including validators, node operators and oracle providers. These functions should be analysed separately rather than treated as a single category. A validator or node operator should not be regarded as interposed merely because it validates, orders, propagates or records transactions in accordance with network consensus rules. Similarly, an oracle provider should not be regarded as interposed merely because it supplies data used automatically by protocol code, although the position may differ where the provider has unilateral control over the data used to determine transaction outcomes or exercises transaction-specific discretion. We ask the FCA to include guidance reflecting these distinctions.

Separately, we ask the FCA to confirm that the existence of technical selection or validation functions within a staking arrangement does not, without more, constitute discretion of the kind relevant to the regulated staking activity or its exclusions. The

analysis should turn on the statutory conditions applicable to staking rather than importing concepts developed for arranging transactions.

Financial promotions (PERG 18.8.34)

PERG 18.8.34 confirms that the technical services exclusion has not been replicated in the financial promotions regime. As a result, a provider that is outside the arranging activity may still be treated as communicating financial promotions merely by displaying information about a protocol, such as rates, balances or supported assets. Where those assets are restricted mass market investments, the resulting requirements cannot in practice be met by an unauthorised interface. This would undo, through the financial promotions regime, the policy that Parliament adopted in article 9Z2A. We ask the FCA to:

(a) work with HM Treasury to align the Financial Promotion Order with article 9Z2A for technical service providers; and
(b) in the meantime, confirm that neutral, factual information (including protocol data, rates, balances and risk information) displayed within an interface in response to a user's own navigation is not an invitation or inducement.

We also repeat our concern, raised in June, about the treatment of stablecoins that are not issued in the UK. Unless its issuer is authorised in the UK, such a stablecoin is treated as a cryptoasset and a restricted mass market investment, and is therefore subject to the full financial promotion restrictions, including the 24-hour cooling-off period for first-time investors and appropriateness assessments. Widely used stablecoins are the main settlement assets of onchain finance. Payment stablecoins issued under the US GENIUS Act must be fully backed one-to-one by reserves of cash and high-quality liquid assets and be redeemable at par. They are distinctly different from cryptoassets whose value is not referenced to fiat currency, and it does not make sense to subject them to the same restrictions. A non-UK issuer may seek UK authorisation, but requiring every issuer of a widely used payment stablecoin to do so before UK users can access it on proportionate terms would fragment liquidity and push UK users towards offshore providers and away from UK-regulated firms. We ask the FCA, working with HM Treasury, to establish mutual recognition of payment stablecoins issued under comparable regimes, such as the GENIUS Act, so that they are treated consistently with UK qualifying stablecoins and are not subject to the financial promotion restrictions that apply to restricted mass market investments. We do not consider that risk warnings alone can offset the effect of rules that restrict access to these assets.

Money Laundering Regulations (PERG 18.8.35)
PERG 18.8.35 confirms that the exclusion does not extend to regulation 14A of the MLRs. We ask the FCA to ensure, with HM Treasury, that a provider of neutral, self-custodial technical access is not outside the arranging activity under FSMA but within the "cryptoasset exchange provider" definition under the MLRs. JMLSG Sector 22 recognises that the application of the MLR cryptoasset exchange provider definition depends on the activities actually performed, including whether the provider exchanges, arranges or makes arrangements with a view to the exchange of

cryptoassets. We ask the FCA to cross-refer to that functional analysis and confirm that the mere provision of neutral, self-custodial technical functionality does not bring a provider within regulation 14A where the provider does not perform any of the activities specified in the statutory definition. The analysis should remain distinct from, but coherent with, the assessment under article 9Z2A.

Terminology and timing
We encourage the FCA to use "self-custodial" rather than "non-custodial" throughout PERG and GC26/7. The term describes what users do, which is to hold and control their own assets, rather than defining the activity by reference to an intermediary that is absent.

We welcome the FCA's statement in CP26/36 that, where uncertainty concerning the technical services provider exclusion has materially affected a firm's ability to submit a complete application during the application period, it will exercise forbearance and allow additional time to address incomplete aspects of the application relating to the arranging permission, provided that the firm submits an otherwise complete application during that period. We ask the FCA to reflect that commitment in the final guidance and to clarify the process by which affected applicants may update the relevant aspects of their applications once the guidance is finalised, without those updates themselves prejudicing the application.

Final guidance is not expected until spring 2027, after the application window closes on 28 February 2027, and after many firms will have had to design their products and arrangements. Article 9Z2A(2)(a) also depends on the status of another firm: it is available only where V is authorised or exempt for the relevant activity. A technical service provider that gives access to a firm whose application has not been determined when the regime commences on 25 October 2027 would lose the benefit of the exclusion through no act of its own, although nothing about its own service has changed. We therefore ask the FCA to clarify, with HM Treasury where necessary, how article 9Z2A(2)(a) will apply during the transition to the new regime where V has submitted an application for the relevant permission within the application window but that application has not been determined by commencement. In particular, A should not lose the benefit of the technical services exclusion solely because the FCA has not yet determined V's application, where V is lawfully permitted to continue the relevant activity under applicable transitional arrangements.

Worked examples
In addition to amending the general guidance, we ask the FCA to include worked examples addressing:

(a) a self-custodial interface that retrieves protocol data, constructs a transaction and transmits a user-signed instruction;
(b) an interface that blocks sanctioned addresses and objectively identified malicious contracts;

(c) a protocol with token-holder governance, timelocked upgrades and a risk steward operating within quantitative limits;
(d) a protocol with a guardian able only to pause new deposits or borrowing during defined emergencies; and
(e) an interface giving access to a protocol that depends on third-party oracle and node infrastructure.

Each example should distinguish: (i) whether the interface provides a technical service; (ii) whether it is "merely" providing that service; (iii) whether the user accesses a third person's services or a decentralised protocol; and (iv) whether any separate participant may itself be carrying on a regulated activity.

Part B: GC26/7

5. General comments

We welcome GC26/7's confirmation that it is non-Handbook guidance that creates no new requirements. We particularly welcome three features:

(a) important business services are identified by reference to the service delivered to clients, not the underlying protocol (paragraphs 3.19 to 3.24);
(b) the guidance contains no mandatory certification or audit regime for protocols. Mandated certification of protocols would amount to regulating them indirectly, and voluntary disclosures, such as security audits, are the appropriate tool; and
(c) the guidance recognises the benefits of DeFi, including automation, continuous access and composability.

We ask the FCA to make clear that firms' due diligence on the protocols they use is the firm's responsibility. It should not translate into de facto obligations on protocols, or on developers that carry on no regulated activity.

Consistency with CP26/36. GC26/7 encourages regulated firms to rely on infrastructure that is maintained and monitored and has effective incident response. It also encourages screening for illicit activity. The perimeter guidance should not penalise the same conduct, by treating maintenance and risk management as indicators of centralisation (PERG 18.8.32) or screening as an indicator of discretion (PERG 18.8.30). The recommendations in section 4 above would align the two documents.

6. Operational resilience (Questions 1 and 2)

We broadly agree with the description of operational resilience risks. We suggest that the guidance also recognise the following mitigants, which firms should assess as part of protocol due diligence and mapping (paragraphs 3.25 to 3.29):

(a) **Protocol-level risk management.** This includes independent risk managers, governance-set risk parameters, onchain monitoring, narrowly scoped guardian or

emergency functions, timelocks on governance changes, audits and bug bounties. These features go directly to the questions firms must answer about incident management and change control.
(b) **Public permissionless blockchains.** Widely used public blockchains have operated continuously through prolonged periods of market stress. They have no single point of failure and broad, independent validator sets, and their transparency allows real-time monitoring by anyone. The guidance should not imply that permissioned networks are inherently more resilient.
(c) **Emerging practices.** These include contributing to, or auditing, critical open-source infrastructure on which a firm depends; maintaining redundant providers (as in the Firm B example concerning RPC providers); and maintaining the ability to restore client services independently.

Outsourcing and dependencies. GC26/7 notes that SYSC 8 applies where a third-party arrangement is outsourcing. We ask the FCA to confirm that reliance on a genuinely decentralised protocol is not, without more, an outsourcing arrangement under SYSC 8. The classification should depend on whether the firm has entered into an arrangement under which an identifiable service provider performs a process, service or activity that would otherwise be undertaken by the firm. Where the firm instead interacts directly with autonomous protocol code and no identifiable person undertakes to provide the relevant service to the firm, the protocol should ordinarily be treated as a technology or infrastructure dependency to be identified, mapped and managed under SYSC 15A and the firm's wider risk-management framework. Any separate contractual arrangements with interface providers, risk providers, node operators or other identifiable service providers should be assessed independently under SYSC 8.

Published risk and listing frameworks. Mature protocols increasingly publish the standards they apply, which gives firms a concrete basis for protocol due diligence and dependency mapping. These frameworks are often developed with independent risk providers and approved through governance. They may cover asset risk (onboarding, periodic due diligence, re-evaluation after material changes, and deprecation), bridging risk, monitoring and chain risk, and can be supported by automated tools that are defensive only: those tools can suspend new activity in a market or lower limits when an adverse signal fires, but cannot loosen them without human review through governance. Technical listing frameworks set consistent requirements that an asset must meet before it is listed and when it is reviewed, covering matters such as verified and audited contracts, reliable price oracles, documented access controls and upgrade authority, timelocks, bridge configuration, bug bounties and disclosure by issuers. Where findings are published with each listing proposal and final decisions rest with governance, firms have a transparent record to draw on. We suggest the guidance recognise published risk and listing frameworks of this kind as evidence that firms can use in their due diligence and mapping.

Protocol-level emergency functions. Some protocols have established guardian functions with narrowly defined emergency powers delegated by governance. These

functions enable designated participants to take precautionary measures, such as temporarily suspending new deposits and borrowing in affected markets, in response to identified security threats or emerging risks. They matter most where speed is critical: a smart contract or bridge exploit, an oracle price failure, or a macro tail-risk event such as a sharp market dislocation or the depeg of a widely used asset. A suspension is temporary and reversible and applies to all users alike. It affects only new deposits and borrowing: users can continue to withdraw and repay, and liquidations continue. Their delegated authority is limited, transparent and subject to governance-defined parameters. Importantly, these guardians cannot seize or transfer user assets or exercise discretion over individual transactions. These safeguards provide a mechanism for responding promptly to threats while preserving the decentralised nature of the protocol. Resilience also depends on the ability to maintain and upgrade the protocol and the blockchain networks on which it runs, so that vulnerabilities can be addressed and protections improved over time. Such upgrades should take place through transparent governance processes subject to timelocks, and should be recognised as part of good operational resilience rather than treated as an indicator of centralisation (see section 4). We suggest that the FCA recognise such bounded, governance-authorised risk management functions as good operational resilience practice, rather than treating them as evidence of centralised control.

Irreversible settlement. The risk analysis in GC26/7 refers to smart contracts that are hard to pause or reverse. Irreversible settlement is a feature of public blockchains: it gives users finality and protects them against arbitrary intervention. The guidance should not imply that firms should prefer protocols in which a person can reverse users' transactions, which would reintroduce the central control and single points of failure that the guidance elsewhere identifies as risks. The appropriate safeguard is the kind of narrowly defined, governance-bounded emergency function described above, which can suspend new activity in an affected market but cannot reverse transactions or move user assets.

Access to DeFi through regulated firms. GC26/7 is premised on regulated firms interacting with DeFi. Its worked examples include a firm that stakes client assets through liquid staking protocols and a wallet provider that relies on decentralised exchange aggregators. However, two requirements in the FCA's Crypto sourcebook could together operate as a de facto prohibition on regulated firms giving their customers access to DeFi protocols. The first is that customer orders be executed only on FCA-authorised venues (CRYPTO 5.2). The second is that retail customers may only acquire assets admitted to a UK trading platform (CRYPTO 5.3.2 and 6.2.3). No authorised person stands behind a decentralised protocol, and the regulatory perimeter applies to persons, not to activities. A transaction executed through a decentralised protocol does not therefore involve a breach of the general prohibition by any person. However, this does not resolve the separate question of how the FCA's intermediary requirements apply where an authorised firm facilitates customer access to such a protocol. Those requirements, rather than the legislation, are the source of the restrictions, and the legislation does not require them. Nor do the public offer provisions require that retail customers be limited to assets admitted to a UK

trading platform, since other exceptions are available and may be relied on in combination.

The question also arises only where a regulated firm holds custody of its customers' assets and gives them access to DeFi from that custodial account. Where customers hold assets in their own self-custodial wallets and independently interact with a protocol, the fact that they previously acquired or withdrew those assets through a regulated firm should not of itself make their subsequent protocol interaction part of the firm's regulated service. The position should turn on the firm's continuing involvement, including whether it recommends or selects the protocol, transmits or executes instructions, controls the interface through which the interaction occurs, receives transaction-linked remuneration, or otherwise facilitates the subsequent transaction. A regulated firm that has delivered cryptoassets to a customer's own wallet, for example following a purchase, is not arranging or executing the customer's later use of those assets, and we ask the FCA to confirm this.

We understand that the FCA does not intend GC26/7 to change existing rules. The FCA has proposed deferring these requirements to 2028. That period provides an opportunity to put a proportionate route in place before they take effect. We therefore ask the FCA to use its existing powers to provide a proportionate route for regulated firms to give their customers access to DeFi protocols, subject to the due diligence, operational resilience and financial crime expectations in GC26/7, clear disclosure when customers leave a regulated environment, and the customer's consent, rather than requiring execution only on FCA-authorised venues and limiting retail customers to assets admitted to a UK trading platform. The issue is not limited to retail cryptoasset trading. As traditional financial institutions tokenise assets, the ability of regulated firms to give their clients access to decentralised lending protocols, for example to use tokenised assets as collateral, will determine whether the UK can host the onchain capital markets that other jurisdictions are now enabling. A proportionate route would be consistent with the approach being taken in the EU, where ESMA and the EBA have supported regulated access to DeFi in the review of MiCA, and in the US. Users should be able to reach DeFi both directly, through self-custodial interfaces, and through regulated firms; neither route should be treated as the preferred path. We also suggest that the Firm B example refer to a "self-custodial" rather than a "non-custodial" wallet provider.

The proportionate route that we refer to above could in our view be implemented through an express rule modification, waiver framework or exclusion from the relevant execution-venue and asset-admission requirements where the firm can demonstrate that:

(a) the protocol satisfies documented due-diligence criteria concerning governance, smart-contract security, oracle dependencies, liquidity, asset risk, incident response and financial crime controls;

(b) the firm clearly discloses that execution will occur through a decentralised protocol rather than an FCA-authorised trading platform and identifies the protections that will not apply;

(c) the customer gives specific consent to that execution method;

(d) the firm has controls addressing price, slippage, front-running and maximal extractable value, failed transactions and protocol incidents; and

(e) the firm monitors the protocol and can suspend new customer interactions where its documented risk thresholds are exceeded.

The FCA could initially permit this through a controlled or limited route pending the 2028 commencement of the relevant requirements, rather than leaving firms unable to design compliant access models before those requirements take effect.

7. Financial crime (Questions 3 and 4)

We broadly agree with the description of financial crime risks. We suggest the guidance also recognise that public ledgers allow funds to be traced to a degree that is not possible in traditional finance, and that interfaces and analytics providers can screen addresses in real time.

Lessons from recent incidents. Security incidents have shown how quickly stolen assets can move across venues and protocols. We support continued work, led by industry and supported by the regulator, on information sharing and on controls at the level of regulated firms and market participants. Such measures should be developed with care. Protocol-level responses should remain bounded, objective and applied to all users alike, including where emergency measures are necessary to contain risks arising from an incident affecting a protocol. Rules requiring decentralised protocols to intervene in individual transactions would reintroduce the discretion and single points of failure that the technical services exclusion and the decentralised protocol limb assume are absent.

Travel Rule and self-custodial wallets. We agree that firms must comply with regulation 64 of the MLRs where it applies. Its application to transfers to and from self-custodial wallets should remain risk-based and proportionate, consistent with JMLSG guidance. Firms should be able to rely on the information available to them and on risk-based measures, rather than being expected to verify the ownership of every self-custodial wallet with which a customer interacts. Such an expectation would discourage self-custody without reducing financial crime risk.

Stablecoin freezes. Uncertainty remains over the legal basis for issuer freezes, their timing and the process for releasing funds later found to be legitimate. We recognise the FCA's view that this is outside the scope of GC26/7, but ask the FCA to prioritise clarity on these points with HM Treasury and law enforcement.

Unidentified counterparties. We ask the FCA to address how exclusions that depend on the identity of a counterparty, such as those for dealing as principal, apply where counterparties in onchain trading cannot be identified.

8. Other risks and mitigation (Questions 5 and 6)

Question 5. One risk the guidance does not address is regulatory displacement. If UK firms and interfaces cannot offer protective features without losing the benefit of exclusions, or cannot give UK users access to widely used assets and protocols, UK users will use offshore services that offer fewer protections. We ask the FCA to take this risk into account in finalising both CP26/36 and GC26/7.

Question 6. Measures that would reduce financial crime risk in DeFi include:
(a) recognising interface-level screening as a valued control, consistent with section 4 above;
(b) public-private channels for sharing information about exploits and illicit addresses in real time;
(c) FCA support for industry-led incident coordination; and
(d) voluntary industry standards on disclosure of security audits and risk management practices.

9. Conclusion

Aave Labs supports the FCA's objective of a clear, proportionate perimeter that protects consumers and market integrity while allowing open, onchain infrastructure to develop in the UK. The two consultations can work together to that end. Our central point is a simple one: the features that make DeFi safer, such as maintenance, risk management and screening, should not be the features that bring it within the perimeter.

In practical terms, the changes that matter most are a positive, functional explanation of what makes a service technical (PERG 18.8.27), and an approach to the decentralised protocol limb that gives it the practical effect HM Treasury intended, by asking whether anyone controls or operates the protocol (PERG 18.8.32). Clear guidance on these points matters most to developers and interface providers who conclude that they are outside the perimeter and will rely on PERG to confirm it. We also ask the FCA to provide a proportionate route for regulated firms to give their customers access to DeFi, so that UK users are not pushed towards offshore services that offer fewer protections.

We would be pleased to discuss any aspect of this response.

Sincerely,

Linda Jeng
Chief Legal & Policy Officer
Aave Labs