



the payments association

Modernising Payment Services Regulation

Consultation on updating the UK regulatory framework for payment services, electronic money and Open Banking

HM Treasury

Published 14 July 2026

Response from
The Payments Association

Introduction

The Payments Association (“TPA”) welcomes the opportunity to respond to HM Treasury's consultation on Modernising Payment Services Regulation, published on 14 July 2026 and closing on 6 October 2026. The consultation is the most significant review of the UK's payment services and electronic money framework since the Payment Services Regulations 2017 (“PSRs”) and the Electronic Money Regulations 2011 (“EMRs”) were made. It will decide where regulatory detail sits in future, how tokenised money and AI agents enter the payments perimeter, and how the next phase of Open Banking is governed and paid for. Our members have engaged with it accordingly.

This response reflects views expressed by TPA members and industry experts through a dedicated members' evidence session held on 15 September 2026, attended by more than 25 members, together with follow-up written submissions, including detailed papers on the legislative architecture and on prudential risk management at payment and e-money institutions. TPA's membership spans banks, payment institutions, e-money institutions, Open Banking providers, card schemes, acquirers, platforms, technology providers and their legal and other advisers, and holds a correspondingly diverse range of views. This response therefore cannot and does not claim to represent the position of every member on every question. Where members hold coherent but different views, most notably on senior manager accountability and on Open Banking pricing, we set out both.

We are grateful to the contributors to this response, which has been drafted by Robert Courtneidge and Natasha Healy on behalf of TPA's Policy team. We would also like to thank HM Treasury for its continuing engagement with industry. We hope this response supports the shared goal of ensuring the UK remains the best place in the world for payments businesses to establish, invest and grow.

The consultation asks 42 questions across Chapters 2 to 4. We answer each of them below, in order and in HM Treasury's own wording, grouped under the consultation's chapter and section headings. Where our members did not have specific evidence on a question, we say so and give a shorter answer rather than speculate.

The Payments Association is content for HM Treasury to identify it by name as a respondent to this consultation.

Emma Banymandhub
CEO
The Payments Association

Executive summary

The Payments Association's five tests for payment services reform

Before drafting detailed responses, TPA convened a members' evidence session to test HM Treasury's proposals against five tests that our members identified as the most consequential. Members refined the tests during the session, adding transparency to proportionality, realism to transition timelines, and a clearer statement that the UK should use its freedom to lead rather than follow. The tests frame our detailed answers and underpin the five recommendations in our conclusion.

- **Proportionate and transparent.** Rules should be proportionate to the risk of the activity and, where relevant, to the scale of the firm. Moving detail from statute into FCA rules must not become a route to tightening it without proper scrutiny, and firms need a clear, timely route to clarification where rules are ambiguous.
- **Future-ready and technology-neutral.** The framework should accommodate tokenised deposits, stablecoins, programmable and agentic payments without repeated primary legislation, by regulating the activity and its risk rather than the technology that carries it.
- **Open and contestable.** New FCA powers over Open Banking interfaces, schemes and pricing should support competition among ASPSPs, PISPs, AISP and new entrants, not gatekeep it.
- **Certain, realistic and cost-aware.** Firms need clear and realistic transition timelines and a real cost-benefit case before statutory certainty is traded for rule-making flexibility. Urgent fixes should not wait for the full rewrite. Regulatory certainty is also what sustains investment in UK payments.
- **Internationally competitive.** Alignment with the EU and other jurisdictions should be a deliberate, case-by-case choice. The UK should go further where that delivers better outcomes, and align where outcomes depend on it, for example in fighting fraud and preserving SEPA access.

These tests inform the five recommendations set out in full in our conclusion: keep legal certainty where it matters and put guardrails on delegation; fix today's tokenised payment barriers now rather than in 2028; regulate by activity and risk, not technology; make agentic payments accountable by design; and give Open Banking a sustainable commercial model backed by enforceable standards.

General observations

TPA members broadly support the direction of HM Treasury's proposals: more of the detail held in FCA rules that can be updated as the market changes, and explicit room for tokenised and agentic payments. Members do not, however, read the proposals as a reason to bring payment and e-money institutions within Part 4A of FSMA, and would not support that. Our evidence session identified several cross-cutting themes that apply across many questions, which we set out here before turning to our detailed answers.

Regulate outcomes and activities, not infrastructure

Members were clear that the reform should start from the economic activity the UK wants to support and the outcomes it wants to secure, rather than from the rail or technology used. A stablecoin, a tokenised deposit or a programmable payment is another way of moving value. If the risk is the same, the regulation should be the same; new permissions or rules should follow only where a demonstrably different risk exists. This is the most effective way to avoid rewriting the framework each time a new technology appears.

An unprecedented opportunity to redesign the perimeter

The consultation is the first real chance since the PSRs were made to look at the perimeter from first principles. Members advising platforms and marketplaces reported that, depending on structure, a single business model can fall within two or even three payment services, or within none of them through available exclusions. Re-wording today's provisions would, in our members' view, result in a missed opportunity. The explicit aim of perimeter reform should be to give firms certainty about what does and does not require permission, and which permission applies.

Sequencing: urgent problems should not wait for the full rewrite

Members understand that the full framework is unlikely to be in force before late 2028. Some of the problems the consultation identifies are live now, in particular the remaining custody permission barrier for firms receiving stablecoin payments on behalf of merchants, which the new exclusion for holding UK qualifying stablecoins temporarily in connection with a payment transaction narrows but does not remove (see Question 7), and the absence of any recognised jurisdiction decisions for overseas stablecoins, whether denominated in sterling or another currency. Members already see clients planning to develop and launch stablecoin payment products from outside the UK, for use by UK customers, because of this uncertainty. Most members urge HM Treasury to separate these items from the wider programme and act on them now wherever they do not depend on the rest of the reform. We made the same point in our response to the Bank of England's consultation on its draft Code of Practice for systemic stablecoin issuers. Some members, including bank members, do not consider that the stablecoin framework should be accelerated ahead of the wider reform.

Transparency and a route to clarification

Delegation to the FCA is generally only an improvement if firms can get timely answers when rules are unclear, though we recognise the speed and flexibility that delegation brings. Members recalled questions put to the European Banking Authority under PSD2 that remain unanswered years later. Members also asked that new expectations be written down rather

than introduced through thematic reviews. Payment and e-money firms are increasingly asked to meet expectations, particularly on prudential risk management, that appear first in supervisory correspondence or multi-firm reviews rather than in published rules. A published standard lets firms price compliance into their business plans at authorisation, rather than retrofit it after supervisory contact.

Regulatory capacity and the burden of regulation

The FCA is already absorbing the Payment Systems Regulator and new responsibilities for cryptoassets, stablecoins and Open Banking under the Data (Use and Access) Act 2025 (“DUAA”). Members want an effective regulator, not an overloaded one. Each proposal to delegate a function or create a power should be assessed against the FCA's capacity to exercise it well, and against the Government's stated ambition to reduce the administrative burden of regulation by 25%. HM Treasury should sequence the delegation of functions to the FCA so that the regulator remains effective throughout the transition, and the FCA should put in place a standing process for maintaining and updating the payments rulebook, so that the agility that justifies delegation is realised in practice.

A joined-up programme

This consultation must be coordinated with the Bank of England's Retail Payments Infrastructure Board work on future retail payments infrastructure, the National Payments Vision and the Payments Forward Plan's aim of streamlining the regulatory landscape, and the Bank of England and FCA's systemic stablecoin regime. TPA has responded to each of these, and we cross-refer to those responses where relevant.

Engagement

Engagement with this consultation has been strong: more than 25 members attended our evidence session, around a dozen contributed directly to discussion, and further written submissions were received ahead of this draft. We would welcome continued dialogue with HM Treasury and the FCA as proposals develop, including through the TPA's working groups.

Response to the consultation questions

HM Treasury's consultation poses 42 questions across Chapters 2 to 4. Each is reproduced below and answered in order. Our answers draw on our members' evidence session of 15 September 2026 and on members' written submissions.

Chapter 2: Approach to updating existing regulatory requirements

Q1: Which requirements should remain in legislation, and which should be delegated to the FCA? Please explain your reasoning.

We support moving most firm-facing requirements into FCA rules, provided the architecture keeps legal certainty where it matters. By this we mean the rule-making architecture that FSMA uses, not bringing payment and e-money institutions within Part 4A of FSMA: firms should remain authorised and registered under a dedicated payments and e-money regime. The test we applied is whether, on balance, delegating a provision would make it easier to keep up to date, or mainly easier to tighten without the scrutiny such a change deserves.

Should remain in legislation. The provisions that decide whether and how a firm is regulated, and the core rights and obligations between payment service providers and their users, should stay in statute. In our members' view that means: the regulated activities, exclusions and key definitions that set the perimeter; the conditions for authorisation and registration; the fundamental allocation of rights and liabilities between payment service users and providers, including consent, the refund right for unauthorised transactions and liability for defective execution; the core statutory protection of customer funds on insolvency; the Open Banking definitions and rights of access that set market boundaries; and the fundamentals of critical third party oversight, given firms' growing dependence on cloud and other technology providers. We also ask that the principle that payments must be authenticated remains in legislation. We support the Government's commitment to revoke the Strong Customer Authentication provisions so that the FCA can make outcomes-based rules, but the principle itself underpins consent in card, remote and Open Banking payments and should not depend on rules alone.

Three further elements should, in our view, stay in statute because they are perimeter questions in substance: the small payment institution and small e-money institution regimes; the provisions allowing payment services to be provided through agents and e-money to be distributed through distributors; and the core safeguarding provisions. On safeguarding, the courts have clarified how the statutory provisions operate on insolvency, including in the *ipagoo* and *Allied Wallet* cases, which confirmed that they do not create a statutory trust. Moving the core provisions into rules risks unsettling that body of law.

Should be delegated to the FCA. Detailed technical and operational requirements, particularly those likely to need updating as the market develops, belong in FCA rules. Examples include safeguarding methodology, reconciliation, segregation and record-keeping; information and disclosure requirements; the technical standards for authentication; reporting; operational detail for critical third parties; and prudential calculation and risk management requirements (see our answer to Question 20).

Guardrails for delegation. Delegation should come with four safeguards. First, the transfer of existing requirements into the Handbook should be a policy-neutral restatement, with any

change of substance consulted on separately with a full cost-benefit analysis. Second, firms need a formal and timely route to clarification where FCA rules are ambiguous. Third, rules should be proportionate to the risk of the activity. Where scale is relevant, it should affect how intensively a requirement applies, for example the frequency of audits or reconciliations, not whether a firm is subject to it. That is preferable to applying one standard to all firms as, in many members' experience, recent safeguarding changes have done. Some members, including bank members, consider that regulation should follow activity rather than firm size. Fourth, firms need realistic implementation periods for significant changes.

Two further points follow. First, the PSRs and EMRs work well partly because they sit in two self-contained instruments, supported by a single FCA Approach Document that firms and other regulators regard as a model of accessible guidance. If the requirements are dispersed across several Handbook sourcebooks, the regime could become harder to navigate, particularly for smaller firms without large compliance teams. We ask that the FCA maintain a single consolidated guide for payment and e-money firms. Second, delegation transfers policy-making from Parliament to the regulator. HM Treasury should set out how FCA rule-making for payments will stay aligned with the programme's own objectives of innovation, competition and proportionality, and what accountability framework will apply.

Q2: Where you consider requirements should remain in legislation, are there any updates you believe need to be made to these requirements?

Yes. Our members identified three areas where the statutory provisions need updating, beyond the definitional points in our answer to Question 3.

The perimeter itself. As set out in our general observations, the reform should aim explicitly to give firms certainty about which activities require permission and which permission applies. Platform and marketplace models are the clearest example: depending on structure, one business can fall within two or three payment services, or within none. We ask HM Treasury to review the perimeter from first principles rather than amend today's wording, and to publish worked examples for common platform, marketplace and embedded finance models alongside the new legislation.

The technical service provider exclusion. It is not clear at what point a technical service becomes part of the payment service itself. The question is increasingly difficult given the range of services such providers offer, including tokenisation, fraud decisioning, payment routing, settlement technology and technical wallet or ledger infrastructure. Clearer statutory boundaries, supported by FCA guidance, would help both providers and the regulated firms that rely on them.

Consent, authorisation and authentication in agentic and other delegated payments. We ask HM Treasury to define these three concepts separately in statute, so that the framework can say who is responsible when a payment is made under delegated authority. When a customer delegates authority to an agent to make payments up to a set amount under pre-defined rules, it is not clear under the PSRs who bears liability when one of these elements fails: whether consent was validly given, who authenticated it, or whether each later payment was properly authorised. This matters for agentic payments (Question 15) and programmable payments (Question 12) and should be resolved at the statutory level, since it determines where liability falls. Firms also need clear statutory definitions and guidance to distinguish genuinely unauthorised transactions from first-party fraud and payments made under a

fraudster's influence, particularly where a disputed payment was executed through an authenticated device or stored credential.

Access to bank accounts. Nearly a decade after the requirement for proportionate, objective and non-discriminatory access to banking services was introduced (regulation 105 of the PSRs), payment and e-money firms are still refused or lose accounts on the basis of banks' commercial risk appetite. This is a barrier to entry, a source of concentration risk and, increasingly, a constraint on cryptoasset and tokenised payment firms too. We ask HM Treasury to strengthen regulation 105 by: giving authorised payment firms a clear right of access, with the FCA able to intervene where access is refused; placing a higher burden on banks to justify refusal to a regulated payment firm; setting timelines for decisions on applications and a minimum notice period for termination, with access maintained until a replacement account is in place; and requiring banks to report, and the FCA to collect and publish, data on refusals and closures.

Safeguarding at the Bank of England. We support acceleration of the Bank of England's work to allow authorised non-bank payment service providers to safeguard customer funds in central bank accounts, and ask that access be widened, and remunerated, on terms closer to those available to banks. This would reduce the concentration risk created by the small number of banks willing to hold safeguarding accounts, reduce operational risk and strengthen consumer protection. Access should not be conditional on a skilled person review under section 166 of FSMA. Firms already obtain annual safeguarding audits, and the cost of a section 166 review would put access out of reach for many of the smaller firms that would benefit most.

FCA discretion over own funds. The FCA can direct which own funds calculation method a firm uses, or require own funds up to 20% higher than the calculated amount. In practice, this creates uncertainty at authorisation. The criteria for these directions should be published and proportionate to the risks a firm actually runs, and any uplift should be time-limited and reviewed for release. This is part of the wider case for published prudential standards that we set out under Question 20.

Q3: Do current provisions relating to the regulatory framework for payment services and electronic money, such as key definitions, need to be updated? If so, please explain how.

Yes. Members reported that several definitions in the PSRs and EMRs are unclear in practice, and that interpretation differs between firms. The main areas raised were:

- **Funds.** The definition of funds (banknotes and coins, scriptural money and electronic money) should be updated so that it clearly includes qualifying stablecoins and tokenised deposits. This is the simplest way to deliver the Government's aim of one set of rules for tokenised and conventional payments.
- **Payment account.** The definition should say clearly how it applies to e-wallets and newer products, and should distinguish payment accounts from technical accounts, ledgers and other arrangements that record value or facilitate transactions without giving the holder payment account functionality. This distinction matters more as platforms, wallets and tokenised arrangements develop. The definitions should also address pass-through and in-device digital wallets, where stored or tokenised

credentials can obscure the funding source and make rapid movements of funds harder to trace and verify against the customer's intent.

- **Payment instruments, orders and transactions.** Definitions of payment instruments, payment orders and payment transactions should similarly be tested against emerging payment models. They should be broad enough to accommodate digital wallets, tokenised deposits, programmable payments and other methods of initiating payment transactions, and should not assume that a payment instruction will always be initiated directly by a natural person or through a traditional payment method.
- **Multi-firm payment chains.** Payment models now routinely involve more than one regulated firm. The framework should recognise these models and make clear how responsibilities are allocated between the firms involved. That allocation should follow each firm's actual customer relationship and degree of control, not the status of a party elsewhere in the flow. Merchant acquiring is the clearest example: the acquirer's customer is the merchant, not the payer, and card payments involve schemes, issuers, processors and payment facilitators whose decisions the acquirer does not control. Consumer protection obligations, including under the Consumer Duty as payments rules move into the FCA Handbook, should be scoped on that basis, as we set out in our response to the FCA's consultation CP26/23.
- **Euro-denominated thresholds.** Thresholds and amounts still expressed in euros should be reviewed and, where appropriate, restated in sterling. However, changes to thresholds may affect the definition of a micro-enterprise. Any change should be assessed for its consequences, to avoid a cliff edge for firms that currently benefit from the protections given to micro-enterprises.
- **Safeguarding terminology.** Certain safeguarding terms, such as when funds are "received", what counts as "relevant funds" and how the obligation applies to funds in transit along a payment chain, are interpreted differently across the sector and would benefit from clearer definition. Merchant acquiring shows the problem most clearly. The safeguarding rules are built around the receipt of cash, but acquirers operate on entitlements: the obligation to the merchant is recorded when a card transaction is cleared, while the cash arrives from the card schemes some days later. One member suggests a safeguarding approach specific to merchant acquiring, based on entitlements on an accruals basis, so that the legal requirement matches how the business operates.
- **Prudential terminology.** Payment and e-money institutions are increasingly asked about concepts drawn from the investment firm regime, such as internal capital and risk assessments and liquid asset thresholds, which do not appear in their own rules. Prudential expectations should use consistent, defined terms and be set out in published rules (see Question 20).

Any change to definitions must be made carefully so that it does not unintentionally move the perimeter or change firms' existing permissions. Members have identified further definitional issues in the PSRs and EMRs, and we would be glad to share these with HM Treasury in detail as drafting progresses.

Q4: Which international regulatory developments, for example recent reforms in the EU, should the UK incorporate into an updated framework for payment services and electronic money?

The EU's PSD3 and Payment Services Regulation are a useful reference point, but should not be the starting template from which the UK departs case by case. Our members' view is that the UK should adopt international developments case by case, where they deliver better outcomes, and go further than the EU where it can. A regime agreed across 27 Member States tends towards the lowest common denominator. The UK led the world on Open Banking by moving first, and agentic payments are a similar opportunity.

There are, however, areas where alignment protects outcomes that matter to UK consumers and firms:

- **Fraud and online platforms.** Fraud is international, and losses remain at unsustainable levels. UK Finance reports that £1.28 billion was lost to fraud in 2025, up 4% on 2024, and that 66% of authorised push payment fraud cases originated online. Under the agreed EU PSD3 and Payment Services Regulation package, online platforms that are informed of fraudulent content and fail to remove it will be liable to payment service providers that have reimbursed defrauded customers. If the EU places these obligations on platforms and the UK does not, consumer protection will become uneven and fraud will migrate to the UK. The UK should at least match the EU's expectations of platforms. We welcome the planned consultation on changes to the UK's APP reimbursement requirements and Ofcom's consultation on strengthening fraudulent advertising codes, and ask that these next steps be taken forward at the earliest opportunity, with any divergence from the EU on PSP liability for fraud and scam losses a deliberate choice rather than an accident of timing.
- **SEPA access.** Many UK firms and their customers depend on continued access to the SEPA schemes, which rests on the UK framework remaining equivalent in relevant respects. Continued SEPA participation should be an explicit objective of the reforms, and HM Treasury should carry out a dedicated assessment of which elements of the EU's PSD3 and Payment Services Regulation the UK framework must reflect to preserve it.
- **Access to device NFC for digital wallets.** We note that the EU has taken several steps to promote access to mobile device functionality used for payments, including requirements and commitments that support interoperability and fair access to NFC-enabled payment capabilities. The UK should consider whether the modernised payments framework should include a requirement on mobile device manufacturers to provide wallet providers with fair, reasonable and non-discriminatory access to payment-enabling hardware and software functionality. However, if the CMA achieves equivalent outcomes through its digital markets powers, additional payments-specific regulation may not be necessary. Greater access would support competition and innovation in account-to-account payments, digital identity services, and alternative wallets and credentials.
- **ICT third-party contracts.** We would not support importing the wider prescriptive approach of the EU's Digital Operational Resilience Act, since the UK's outcomes-based operational resilience framework gives firms more appropriate flexibility. DORA's minimum contractual requirements and use of standard contractual clauses

for ICT third-party providers could, however, reduce the time firms and providers spend negotiating regulatory terms.

- **Transparency of AI-generated content.** The EU AI Act's requirements for AI-generated content to be identifiable, and for deepfakes to be disclosed, are relevant to identity verification, fraud and impersonation risk in payments. HM Treasury could consider whether similar, proportionate transparency principles would help firms' KYC and fraud controls, without discouraging firms' own use of AI.
- **Stablecoin regimes.** The recognised jurisdiction test for overseas stablecoins will in practice turn first on the EU's Markets in Crypto-Assets Regulation and the US federal stablecoin regime. We address this under Question 6.

Chapter 3: Responding to new developments in payment services

3.1 Supporting tokenised payments

Q5: Does the current regulatory framework need to adapt to unlock the opportunities arising from the use of tokenised deposits in retail payments?

Yes, in a targeted way. A tokenised deposit is a deposit, and the bank issuing it already holds the relevant permissions. The adaptation needed is to the payment services rules that sit around it, so that they work for tokens settled on distributed ledgers: how the payment account definition applies to token wallets, when a payment order is received and becomes irrevocable, execution time in a system that settles 24 hours a day, and how error correction works where settlement is final on the ledger. Our answers to Questions 12 and 13 cover these points.

Members asked what evidence would show that tokenised deposits are ready for retail payment journeys beyond pilots. In our view, HM Treasury and the Bank of England should look for four things: interoperability between different banks' tokens so that they are exchangeable at par; access for non-bank payment service providers on fair terms; consumer protection equivalent to conventional deposit-based payments; and settlement arrangements coordinated with the Retail Payments Infrastructure Board's work. Tokenised deposits and stablecoins should be regulated on a technology-neutral basis for the payment activity they support.

Q6: Do you agree that only stablecoins issued in the UK or from a 'recognised jurisdiction' should be treated as 'money-like' for the purposes of payments, and brought into the UK payments perimeter?

We broadly agree, subject to one condition that most of our members regard as urgent. The recognised jurisdiction test must be transparent, predictable and quick to operate. It must not become a hidden barrier to entry. Some members, including bank members, do not consider that the stablecoin framework should be accelerated ahead of the wider reform.

Speed must not mean a lower bar. Recognition should rest on outcomes-based equivalence, including redemption at par, high-quality backing assets held for the benefit of holders and independently verified, prudential and supervisory arrangements proportionate to the issuer's scale and systemic significance, effective financial crime controls and a credible insolvency framework. A money-like instrument should not operate at scale in the UK to a materially lower standard than commercial bank money.

In practice, the first candidates for recognition will be the EU and the US, possibly followed by Singapore and some Gulf states, and work on this is already underway through the UK-US Transatlantic Taskforce for Markets of the Future. The most widely used stablecoins for payments today are US dollar stablecoins. Members report that clients are already planning to run stablecoin payment products from outside the UK into the UK, because they expect to use those coins and have no certainty that they will ever be treated as money-like here. Every month without a decision moves more of this activity offshore.

We therefore ask HM Treasury to publish the recognition criteria and process now, and to take decisions on the EU and US regimes as soon as feasible, independently of the wider legislative timetable. We also ask for clarity on how payments made with stablecoins that are not treated as money-like will be characterised, so that firms supporting them know which regime applies. This connects with the level playing field concern we raised in our response to the Bank of England's draft Code of Practice for systemic stablecoin issuers.

Q7: Should firms authorised to issue 'UK-issued qualifying stablecoins' be allowed to provide payment services without additional permissions, but be subject to relevant requirements?

Yes, subject to relevant requirements, but for a different reason from the one the consultation gives. The closer analogy is not a bank, which provides payment services on deposits it already holds, but an e-money issuer: the stablecoin issuer issues the monetary value that is then used to pay. Electronic money institutions can already provide payment services under their authorisation, subject to the payments conduct and safeguarding rules, and the same approach can work for authorised stablecoin issuers. Issuers should, however, have to demonstrate payment-specific capabilities, including fraud prevention, transaction processing, sanctions screening, customer protection and operational resilience, before providing payment services at scale, for example through notification to and assessment by the FCA rather than a full new application. Some members would go further and require a separate permission.

Issuers are also not usually the firms that move stablecoin value in practice. That role is typically played by wallet providers, exchanges and firms that look much like today's acquirers. If the aim is to avoid duplicative applications, the same principle should extend to firms authorised under the new cryptoasset regime to hold or transfer qualifying stablecoins for customers, subject to the relevant payments conduct and safeguarding requirements.

There is a related and more immediate problem. When the new cryptoasset regime commences, a payment firm holding stablecoins for customers will need a Part 4A permission for safeguarding cryptoassets unless an exclusion applies. The exclusion for holding UK qualifying stablecoins temporarily in connection with a payment transaction helps, but it is narrow: the FCA's guidance indicates that "temporarily" is unlikely to extend beyond about 24 hours, and it does not cover overseas stablecoins, which are the coins most used for payments today. Firms accepting stablecoin payments for merchants, or offering wallets or stored value, therefore face a significant barrier before this reform could take effect. We ask HM Treasury to deal with it separately and now, for example, by widening the exclusion for payment firms pending the move of stablecoin safeguarding into the payments regime (Question 8).

Q8: Do you agree that safeguarding of UK-issued qualifying stablecoins, where that is within new article 9M RAO, for the purposes of payments should eventually be regulated under the payments regime and not the cryptoassets regime?

We agree with the destination, since one safeguarding regime for payment activity is simpler for firms and clearer for customers. Stablecoins used for payments are funds used for payments, and a payment or e-money institution already safeguarding customer funds should be able to safeguard them under the payments regime in broadly the same way. This follows from technology neutrality: stablecoins and tokenised deposits used for payments are another form of relevant funds, and the safeguarding obligation should attach to funds received for a payment, whatever form of money they take. It should be done directly: payment firms should not have to obtain a Part 4A cryptoasset safeguarding permission, either permanently or as an interim step, simply because they use stablecoins, and the move should not become a route to bringing payment services within FSMA. HM Treasury should publish the transition path and timetable early, provide an interim solution for the gap described under Question 7, and coordinate with the Bank of England's safeguarding arrangements for systemic stablecoins so that a firm growing to systemic scale is not moved across three regimes.

Q9: Do you agree with the proposed broad split of regulated activities for payments and electronic money issuance?

Yes. The specific changes proposed, combining the placing and withdrawal of cash with the operation of a payment account, combining execution with and without a credit line, and separating issuing payment instruments from acquiring payment transactions, make sense. We ask for five assurances.

- **No loss of existing permissions.** Firms should be mapped automatically to the new activities and should not have to reapply for activities they are already authorised to undertake, including issuing firms whose permission will now sit under a separate activity.
- **No change to risk obligations.** Combining activities should simplify permissions without implying that the underlying risks are the same. Cash placement and withdrawal carry different financial crime risks, as does execution covered by a credit line, and firms should continue to assess and mitigate each.
- **E-money issuance remains separate.** Issuing e-money is different from providing a payment service and carries its own responsibilities. It should remain a distinct regulated activity.
- **Cash placement and withdrawal.** The reference to “all operations required for operating a payment account” in the merged cash activity has led to suggestions that firms need that permission simply because they operate a payment account, even with no cash services. The wording should be clarified so that firms do not need two overlapping permissions for the same activity.
- **Equal treatment for account information and payment initiation.** Banks need only notify the FCA to provide these services, while payment and e-money institutions must apply for a variation of permission. The process should be the same for all.

Beyond this, we repeat our general point that the reform is the opportunity to redesign the perimeter from first principles. The same activity should not be capable of being treated as

two different payment services requiring two permissions, as some European regulators have concluded.

Q10: Do you agree with the proposal to have a single set of regulated payments activities for both tokenised and non-tokenised payments? Are there any risks associated with combining activities in this way? If so, should these risks be mitigated by framing regulated payment services activities differently?

Yes. A single set of activities reflects the principle our members support most strongly: same activity, same risk, same regulation, regardless of the technology used. It also avoids having to amend the perimeter each time a new form of tokenised value appears.

Tokenised payments do raise some different risks, in particular custody of tokens, settlement finality on a ledger, programmability, and the risk that tokenised credentials or wallets obscure the underlying funding source or identity, degrading real-time fraud monitoring. In our view, these are better mitigated through targeted rules and guidance attached to the specific risk feature, such as wallet security, key management, smart contract governance, or appropriate sharing of transaction and device data between wallet providers and payment service providers, than by framing the regulated activities differently. New activities or permissions should follow only where HM Treasury can point to a demonstrably different risk that rules cannot address. Where it believes such risks exist, we would welcome worked use cases explaining them.

Q11: Do you agree that authorised and registered firms should require a variation of permission to carry out payment services using tokenised payments?

Members were not persuaded that the use of a different technology, on its own, justifies a variation of permission. If a firm is already authorised to execute payment transactions, a change of settlement technology does not change the activity. We would prefer a notification requirement, with an FCA power to object or impose requirements, and a variation of permission only where the firm takes on a genuinely new risk, for example providing custody of tokens for customers as a standalone service, outside the course of a payment transaction. Holding tokens in the course of providing a payment service is safeguarding, and should sit under the payments regime (Question 8) rather than trigger a variation of permission.

If HM Treasury retains a variation of permission, it must be proportionate and quick. Members' concern is that it becomes, in practice, a second full application running on current FCA authorisation timelines. We ask for a streamlined process with published criteria focused on the tokenisation-specific risks, a published target determination period, and a transitional arrangement for firms already providing tokenised payment services lawfully when the new regime commences. The FCA should not implement the requirement by imposing a general restriction at the authorisation gateway barring firms from stablecoin payments until they apply to lift it, since that would undo the principle of one set of activities for tokenised and conventional payments.

Q12: How does the payment services regulatory framework need to adapt to support the use of smart contracts and programmable payments underpinning them?

Our members illustrated the issue with a simple example. A buyer agrees to purchase a bicycle through a smart contract. A deposit is earmarked in the buyer's account but does not leave it. When the buyer and seller meet and the goods are inspected, the contract is

completed, and both the deposit and the balance are released to the seller. Under today's consent and revocation provisions (regulations 67 and 83 of the PSRs), the buyer could in principle withdraw consent up to the point the payment order is received, even after the seller has acted in reliance on the earmarked funds. It is unclear what happens to the earmarked funds, and what redress either party then has.

Members debated whether this is a problem with the payment rules or with how the smart contract is built, since the payment obligation and the underlying contract are already distinct today. Smart contracts are a use case, not a new payment service, and most questions about how existing rules apply can be answered through FCA guidance. The consent and revocation rules are the exception, because they are statutory and guidance cannot change them. We therefore suggest that the framework:

- recognises conditional payment orders expressly, with clear rules on when consent is given, when the order becomes irrevocable and what happens to earmarked funds if conditions are not met;
- sets execution time and value dating from the point the conditions are satisfied, not the point the instruction is created;
- allocates liability for losses caused by errors in contract code, distinguishing the payment service provider's execution from the contract logic supplied by others; and
- builds on existing concepts, such as the provision allowing funds to be blocked with the payer's consent where a card payment amount is not known in advance, rather than creating a separate regime.

All of the consent, authentication and authorisation requirements should be reviewed for their effect on smart contract payments, alongside the redress and customer protection that apply when a programmable payment goes wrong.

Q13: Are the current conduct of business requirements in the payment services regulatory framework suitable for tokenised payments? Please explain your answer.

Largely yes. The existing conduct requirements on information, consent, execution and liability can apply to tokenised payments, and we would not support a separate conduct regime. Firms do need worked examples on points where the literal application of today's rules produces uncertain results, including: execution time and value dating in a system that settles continuously; disclosure of network or transaction fees that vary with ledger conditions; the use of wallet addresses as unique identifiers, and liability for misdirected payments where a ledger transfer cannot be reversed; how refund rights for unauthorised or defective payments are met where settlement is final on the ledger; and consent and disclosure where a payment is governed by programmable logic. These should interact cleanly with the Consumer Duty.

Q14: Are the current prudential requirements in the payment services regulatory framework suitable for tokenised payments? Please explain your answer.

For tokenised payments specifically, broadly yes. Where a firm adds stablecoins to its payment services, they should be treated as funds, and the firm should continue to calculate own funds under the existing methods. Under the payment volume method, for example, stablecoin payments would simply form part of volume. Tokenisation alone should not trigger a separate or additional capital requirement. The FCA should, however, expect firms' risk

management to cover the specific operational risks of the settlement infrastructure they use, including custody and key management.

There is a separate question, not specific to tokenisation, about firms that run material credit, market and liquidity exposures, for example by dealing as principal in foreign exchange forwards. For those firms the current own funds methods, which measure overheads, volume, income or outstanding e-money, are not sensitive to the risks involved. Our answer to Question 20 sets out a targeted proposal for published standards, scoped so that most firms are unaffected.

3.2 Leading the world in agentic payments

Q15: How does existing payment services regulation need to adapt to support agentic payments? For example, do provisions relating to authentication and consent of payment transactions, and liability for unauthorised payment transactions, need updating?

Yes. The central question our members asked is this: if an agent makes a payment the customer would not have authorised themselves, whose liability is it? Many initial agentic use cases can operate within the existing framework. It cannot answer that question clearly, however, especially where consumers choose to delegate more autonomy to agents. The UK has a real opportunity to lead here, but only if accountability is designed in before adoption scales, not after the first large dispute.

From payment authorisation to mandate authorisation. Agentic payments move the point of control from the individual payment to the mandate the customer gives the agent. The framework should recognise mandate-based consent. Consent and authentication captured when an agent is set up should satisfy the authentication requirements only where the mandate's scope, value and frequency limits, permitted merchants or categories, duration and means of revocation are clear, recorded and auditable. Open-ended mandates should not. Mandates may also need to be progressive, for example allowing an agent to place a deposit but not to complete the full purchase without further confirmation. This depends on the statutory separation of consent, authorisation and authentication we propose under Question 2.

Liability should follow role, not default to the payment service provider. Members were clear that liability cannot rest automatically with the customer, the agent provider or the payment service provider. Where an agent acts outside its mandate, the customer in principle already has a right of action against the agent's provider, but in practice few consumers will pursue it. Nor should banks and payment service providers be the backstop for every failure. Members drew a direct lesson from fraud: online marketplaces originate a large share of fraud but carry little of the liability. Agentic commerce should not repeat that pattern. The parties in the chain, including technology providers closely involved in instructing or triggering payments (we do not use "initiating" here in the defined sense of a payment initiation service), should carry responsibility in line with their role from the outset. Not every technology supplier needs to be regulated, but those whose capabilities are closely involved in instructing or triggering payments should face some regulatory scrutiny.

Options for new regulated activities. One option members put forward, and which has been discussed with HM Treasury, is to create two new regulated activities: a mandate assurance

service, covering the issuing, maintenance and attestation of an agent's delegated payment authority; and an agentic payment service, covering a provider that, acting under delegated authority, initiates or causes the initiation of a payment and assumes liability for failures downstream. TPA's Agentic Commerce working group will develop this further, and we would welcome the opportunity to work through it with HM Treasury.

Fraud classification and the ability to intervene. Consent determines whether a disputed agentic payment is treated as unauthorised or as authorised push payment fraud, and therefore who bears the loss. This work should be joined up with the Government's current work on unauthorised fraud. Firms must also keep the ability to delay or stop suspicious payments, including under the powers to delay outbound payments where fraud is suspected. Members discussed an indicator in the payment message showing that an agent was involved, and possibly which agent, so that firms can apply appropriate checks. Any such indicator must be designed so that it does not add the kind of friction that has held back Open Banking adoption. Members were divided on a central registry of agents: it could help contain a compromised agent, but it would create a new body, cost and potential barrier to entry.

Vulnerable customers. Agentic commerce combined with vulnerability creates specific risks, for example a customer with dementia whose agent repeatedly orders the same goods, each order individually authorised and within its mandate. Payment service providers already have obligations to identify and act on known vulnerabilities, and should be able to adapt agentic services accordingly, for example through quantity or frequency limits (see Question 17).

What belongs in law and what in standards. It is early in the adoption of agentic payments, and detailed rules written now risk fitting poorly the models that emerge. In our view legislation should settle the principles: that a mandate can constitute consent, and that liability follows role. The detail, including how agents are identified to customers and payment service providers, how agent-initiated transactions are flagged, and record-keeping and audit standards for mandates, is better developed through FCA rules, guidance and industry standards that can evolve with the market, informed by real-world deployment and a strong evidence base.

Q16: Are there any other innovations across the payments landscape that the Government should take into account when reforming its payment services regulatory framework?

Members highlighted four:

- **AI on both sides of financial crime.** Deepfakes, AI-generated identities and manipulated documents are making identity fraud, impersonation and account takeover more convincing and more scalable. AI also strengthens firms' own detection. The framework should support firms in adopting AI for financial crime controls with appropriate governance.
- **Access to device technology.** Access to NFC and other device functions for third-party wallets and payment apps (see Question 4).
- **Continuous, real-time payments.** Payments now operate 24 hours a day, which changes the pace at which customer balances and firms' liabilities move. Safeguarding, liquidity and fraud controls need to work in that environment.

- **The framework's own ability to adapt.** Members see the most valuable innovation as a rulebook that can adapt quickly to new technologies, with an FCA sandbox and testing capability that lets firms engage early on new models, rather than new rules written for each technology.

3.3 Ensuring financial inclusion

Q17: How can the Government ensure these reforms support an inclusive payments landscape?

By focusing on outcomes and building on the Consumer Duty, not by creating a separate compliance regime. The Consumer Duty and the FCA's guidance on customers in vulnerable circumstances already require firms to consider the needs of different customers, and new requirements would risk duplicating them.

Members asked the Government to distinguish two things that are often conflated: broad inclusion, which is about access for everyone, including older and less digitally confident customers; and protection for customers in vulnerable circumstances, which is a narrower group that overlaps with the first. Technology can help inclusion. Many people who are not digital natives now manage day-to-day finances on a mobile phone or smartwatch, and simpler journeys and more accessible authentication can widen access further.

Nevertheless, we recognise the Consumer Vision for Payments and note that further work is needed to build confidence in, and use of, digital payments. Some 11 million people help others with basic digital banking tasks (industry research, 2024), and disabled people continue to experience inconsistent outcomes when making payments in different situations (AlixPartners, Improving Accessibility in Payments, 2025). Technology offers new opportunities to promote inclusion, and we would support their further development, for example alongside the findings of the independent review into access to banking. We encourage the Government to work with others, such as the Centre for Finance, Innovation and Technology, to provide the consent and trust frameworks that enable third party access for financial helpers, and to build further infrastructure that improves the accessibility of digital payments.

Where the reforms create new risks for vulnerable customers, particularly agentic payments, the framework should allow and expect firms to adapt services for known vulnerabilities, for example by limiting the quantity or frequency of automated purchases, while preserving the customer's autonomy. TPA's Financial Inclusion working group would welcome the opportunity to contribute to this work.

3.4 Managing sector risks

Q18: What are the key risks which have emerged to consumers and businesses in the payments and electronic money sector over recent years, and how well do the current regulations address this?

Members identified five groups of risk:

- **Fraud and financial crime**, including account takeover, identity fraud and authorised push payment scams, made faster and more scalable by digital channels and more

convincing by AI. Real-time payments leave firms less time to identify and stop suspicious payments.

- **Operational and third-party risk**, including cyber incidents and outages at cloud providers, banks and processors that sit outside the firm's direct control.
- **Safeguarding risk** in a 24-hour, real-time environment where firms' liabilities to customers change quickly, and where weaknesses surface only when a firm fails.
- **Prudential and liquidity risk**, particularly at firms that act as principal in foreign exchange forwards or extend credit to customers. The FCA's June 2025 multi-firm review found firms with no risk appetite or risk management framework for credit extended to customers and no link to liquidity stress testing, and noted that FX market turbulence had affected some firms' liquidity. A firm can be fully hedged, solvent and compliant with its own funds requirement, and still fail because margin is called before its client pays.
- **Uneven accountability across the fraud chain**. Much fraud originates on online platforms and telecommunications networks, which face far lighter obligations and liability than payment firms. The comparison between financial services regulation and the treatment of the technology and telecommunications sectors should be part of this review.

The current framework already addresses many of these risks. Before new requirements are introduced, HM Treasury should establish whether a problem reflects a gap in the rules or poor application of existing rules, since the remedy is different. Where a gap exists, most clearly on prudential risk management, the response should be targeted and proportionate (see Question 20).

Q19: Would enhanced accountability of senior managers in the payment services and electronic money sector support better management of financial crime risks? What benefits, costs or risks, including to the UK's international competitiveness, should the Government consider?

Our members hold two coherent but different views on this question, and we set out both.

The first view questions whether an additional accountability regime is needed. Payment and e-money firms are already subject to governance, systems and controls requirements, and the FCA already has powers to act where standards are not met. Members holding this view asked HM Treasury to identify the specific gap a new regime would close, and noted the absence of clear evidence that the existing senior manager regimes have improved outcomes in the sectors where they apply. A new regime is a fixed cost that every authorised firm carries, whether or not it was ever the source of the risk being addressed, and that cost bears on the UK's attractiveness as a place to establish a payments business. If introduced, it should be proportionate to firm size and risk, not the banking Senior Managers and Certification Regime applied wholesale.

Some members holding this view argued that the gap is in board governance rather than in individual accountability. In their experience, FCA expectations on non-executive directors, board independence, board members' qualifications and board effectiveness are much less developed than those of some other European regulators. Stronger board governance could

reduce the need for expanded senior manager liability, because an effective board would do much of that work.

The second view supports enhanced accountability for senior managers of e-money institutions, on the grounds that it would align them with the regime already applied to banks and other financial services firms and create a more level playing field. Members holding this view note that similar divergence exists across the wider industry.

Whichever approach is taken, three considerations should shape it. First, directors and managers of payment and e-money institutions are already assessed as fit and proper under the existing regime, and the FCA can already act where concerns arise. Second, the Government and regulators are part-way through reforming the Senior Managers and Certification Regime itself, with a stated aim of substantially reducing its burden and with the most significant changes dependent on further legislation; extending it to a new sector before its future shape is settled would be premature. Third, the EU's PSD3 and Payment Services Regulation do not include an equivalent individual accountability regime, so a UK regime would add a cost that competing EU locations do not carry. We ask HM Treasury to publish a clear statement of the problem being solved, a cost-benefit analysis that includes the effect on international competitiveness, and a proportionate design that distinguishes small and low-risk firms.

Q20: Are there targeted amendments that could be made to current regulation which would tackle sector risks in a proportionate way?

Yes. The clearest example is prudential risk management. The aim is not more capital across the sector. It is to replace requirements that are currently set bilaterally and unpredictably, through supervisory directions and thematic reviews, with published, proportionate standards that apply only to firms running the relevant risks.

The gap. Schedule 3 to the PSRs sets own funds by reference to fixed overheads, payment volume or a relevant income indicator, and Schedule 2 to the EMRs adds a percentage of average outstanding e-money. None is sensitive to the credit, market, counterparty and liquidity exposures that payment and e-money firms dealing as principal actually run. A firm could double the credit it extends, or the tenor of the forward contracts it writes, without its own funds requirement changing. On liquidity there is no quantitative floor, no definition of eligible liquid assets, no encumbrance test, no haircuts and no currency matching rule. Wind-down planning is required in principle, through the risk management conditions of authorisation and the FCA's Principles, but no rule says what a plan must contain, how often it is reviewed, whether it is stress tested, or that resources for an orderly wind-down must be quantified and held. The only route to a firm-specific, risk-sensitive requirement has historically been an FCA direction following a supervisory issue or thematic review. That is bilateral, not a published standard.

The risks are the same. Where a payment or e-money institution acts as principal in a deliverable FX forward, the MiFID exclusion turns on the client's purpose, not the firm's exposure. The firm typically hedges each client contract with a bank. That creates counterparty credit risk on the client leg and liquidity risk on the hedge leg, because the bank calls margin as soon as the market moves while the client may owe nothing until delivery, or may not pay at all. An investment firm running the same book faces the same exposures. From a risk management perspective, a "means of payment" forward and a MiFID forward are the same.

The proposal. Prudential risk management for payment and e-money institutions should sit in FCA rules drawing on the architecture already applied to non-small and non-interconnected investment firms under MIFIDPRU: an internal capital and risk assessment process, own funds and liquid asset threshold requirements, and recovery and wind-down planning. MIFIDPRU need not apply in full. The risk-to-firm factors that measure market risk (including the structural currency position created by earning in non-sterling currencies), counterparty default on derivatives, daily trading flow and concentration are directly relevant; the risk-to-client factors would need adaptation; the liquidity provisions are equally portable. Existing initial capital and own funds methods could remain as the floor. This is not a request for higher capital across the sector. Firms outside the scope test described in the next paragraph would see no change. For firms within scope, any additional requirement would reflect risks they already run and which the FCA currently addresses through individual directions. HM Treasury and the FCA should assess the capital impact on in-scope firms as part of the cost-benefit analysis before any rules are made.

Proportionality through a scope test. A published scope test, performing the function the small and non-interconnected criteria perform for investment firms, would confirm to most smaller firms that the new rules do not apply to them. Relevant criteria would include: whether the firm acts as principal in deferred delivery FX or other derivatives; the gross notional and tenor of contracts outstanding; the size of its net open currency position, including accrued earnings held in non-sterling currencies; whether it extends credit to customers in connection with margin; the value of customer funds held; and reliance on intragroup liquidity support. Firms below the test would remain subject to existing requirements only.

This can be done now. The FCA applied its Principles to payment and e-money institutions in 2019 using section 137A of FSMA as applied by paragraph 3 of Schedule 6 to the PSRs and paragraph 2A of Schedule 3 to the EMRs. It could use the same power to make prudential risk management rules without waiting for the regime to move into the Handbook. When it applied the Principles, the FCA said it would consider intervening if arrangements proved insufficient. Its 2025 review, in which none of the 14 firms sampled fully met expectations, has since supplied that evidence. Published rules would also level the playing field: firms could price compliance in at authorisation, rather than choosing between building a framework they may not need and retrofitting one after supervisory contact.

Other targeted amendments raised by members were: allowing the recent safeguarding reforms to bed in before further change, while ensuring they work in a 24-hour payments environment; clearer expectations on board governance (Question 19); and greater accountability for online platforms and telecommunications providers in the fraud chain (Questions 4 and 18). The Payment Systems Regulator's analysis of where APP fraud originates confirms the role social media and technology platforms play in recruiting victims, and platforms should be required to play their part, for example through stronger identity checks on those selling or advertising through them. Some members also noted that, unlike authorised push payment fraud, there is no shared liability with receiving payment service providers for unauthorised payments, which weakens incentives on receiving firms to maintain robust mule account controls, and asked HM Treasury to consider whether that liability should be shared across the payment chain. Members support building on the information-sharing provisions of the Economic Crime and Corporate Transparency Act 2023 to enable intelligence sharing across payments, media and telecoms, but are divided on how. Some favour an industry-led approach. Others consider that sharing should be mandatory, because financial

institutions alone cannot see the whole fraud journey, much of which begins on social media and messaging platforms or through SIM-swap, and those enablers should share responsibility. Each amendment should be tested against actual enforcement cases and evidence of harm, not perceived gaps.

Chapter 4: Unlocking the future of Open Banking

Members' views on Open Banking diverge more than on any other part of the consultation, in particular between account servicing payment service providers ("ASPSPs") and third party providers. Where that is the case, we set out the range of views. TPA is also consulting its Open Banking working group on the questions below and may supplement this response.

Modernising foundational Open Banking provisions in the Payment Services Regulations

Q21: Do you agree with the proposal to establish a new right of access to support the development of variable recurring payments? If so, what do you think the scope of this new right of access should be, both in terms of the requirement itself and its scope of application? Please explain your answer.

Yes, in the view of most members. Variable recurring payments are the most important near-term extension of Open Banking, and a statutory right of access provides a floor beneath commercial schemes: the capability must be available, while the terms are for the market. The right should cover the lodging of payment mandates for both sweeping and non-sweeping use cases, with the commercial terms for non-sweeping access governed by the framework discussed under Question 22. It should be framed around mandates rather than a list of use cases, so that it can support new models, including payments initiated by AI agents under a customer's mandate (Question 15). On scope of application, neither a current account test nor a size threshold is durable: many payment and e-money institutions are also ASPSPs, and a size test would catch firms whose accounts attract no third party demand. We suggest ASPSPs be brought into scope on the basis of actual or reasonably anticipated third party demand, assessed by the FCA against published criteria, with a defined implementation period.

Some ASPSP members take a different view. Some favour a more targeted scope, for two reasons. First, proportionality: the right should let industry focus investment on the account types and use cases where customer demand and economic benefit are likely to be greatest, avoiding unnecessary cost and operational complexity. Second, a risk-based introduction: variable recurring payments are an emerging payment mechanism that needs clear rules on liability, fraud prevention, authentication, dispute handling and consumer protection, and a targeted scope would let those arrangements mature in a more controlled environment. Others do not support a statutory right of access at all. In their view, industry-led commercial variable recurring payments are already progressing, with much of the market live and the cross-industry establishment of UKPI, there is no evidence of market failure to justify intervention, and intervention could undermine innovation, investment and the phased development of future use cases and consumer protections. The demand-based scope test we propose above goes some way to meeting the concerns of members who favour a targeted scope.

Q22: What are your views on whether and under what circumstances ASPSPs should be able to charge third party firms for the access which they are currently required to provide for free under the PSRs and CMA Order?

Members' views differ, broadly along the line between ASPSPs and third-party providers. Some members, including third party providers, are concerned that charging could price smaller PISPs and AISPs out of the market. Others argue that only once ASPSPs can be rewarded for access can they reasonably be required to provide materially better APIs. One ASPSP member proposed a single free call per day, with charging thereafter, for both account information and payment initiation services.

Taking both views into account, we propose a clear boundary. Access within the existing rights of access in regulations 69 and 70 should remain free of charge. Charging should be permitted for functionality beyond that baseline, including non-sweeping variable recurring payments, richer data, guaranteed performance and other premium services. This directs investment incentives at new capability rather than at monetising infrastructure already built, protects existing business models, and, as we understand it, broadly matches where the EU has landed in its PSD3 negotiations. We would caution against charging for baseline access by reference to volume: the heaviest users of APIs are often aggregators, whose costs would pass down to the smaller providers that use them, and account information services, which rely on frequent access, would be hit harder than payment initiation.

Where charging is permitted, the quid pro quo should be materially higher API standards. Today, dedicated interfaces need only match the performance of a firm's own website or app, not the standard expected of payment-grade infrastructure. Charged services should come with mandated, monitored and enforceable standards, with consequences when they are not met, and pricing should be fair, cost-reflective and subject to FCA oversight. Sweeping should remain free. We also ask HM Treasury to set out the criteria and timetable for any FCA power to move currently free access to a commercial basis: an open-ended power, exercisable at an unspecified time on unspecified grounds, is itself a deterrent to investment in Open Banking today.

Q23: Are there circumstances in which you think the ban on ASPSPs requiring a contract in regulations 69 and 70 should be lifted?

No, for baseline access. The ban removed a significant barrier to entry and should remain in place for access required under regulations 69 and 70. A contract would transfer to the ASPSP control over not only price but data fields, permitted use cases, onward data sharing and termination, any of which could undermine established business models. Contracts are appropriate only for premium functionality accessed through a commercial scheme whose rulebook the third party provider has chosen to join.

Q24: Are there adjustments that should be made to the Rights of Access as set out in regulations 69 and 70 of the PSRs which would better support Open Banking?

Members' priorities are enforceable performance standards for dedicated interfaces, covering availability, response times and conversion parity; clear and quick dispute resolution when interfaces underperform; and clarity about where each Open Banking obligation sits. Requirements are currently spread across the CMA Order, FCA rules, the PSRs and, in future, rules made under DUAA. As Open Banking moves into its next phase, firms need one clear statement of the framework.

Q25: Are current definitions in the PSRs which are relevant for Open Banking, for example definitions of payment initiation service or account information service, fit for purpose? Please explain.

Broadly, but they should be updated for clarity without being redrawn in ways that change scope by accident. The priorities are: to confirm whether lodging and managing a mandate for variable recurring payments is, or is part of, a payment initiation service; to clarify that the payment service user for payment initiation may be the payer or the payee, depending on the proposition; to clarify when a provider of AI tools is providing account information or payment initiation services rather than supplying technology; to consider framing account information services around authorised access to account data rather than the provision of consolidated information; and to define “accessible online” and “sensitive payment data”, both of which have produced inconsistent interpretations and, in some cases, ASPSPs withholding data third parties are entitled to. Any change should be tested against real disputes and implementation friction that members report, not theoretical gaps.

Q26: Are there any requirements related to Open Banking within the PSRs that you consider should remain in legislation, as opposed to responsibility for the requirement being given to the FCA?

Yes. As a principle, requirements that confer a right or protection on a market participant or user should stay in legislation, while technical and operational obligations move to FCA rules and Future Entity standards. That means keeping in legislation: the definitions that set market boundaries; the rights of access in regulations 69 and 70, including the new right for variable recurring payments; the prohibition on requiring a contract for baseline access; the principle of what may and may not be charged for, as distinct from the level of any charge; the allocation of liability between ASPSPs and third party providers; and the principle that payments must be authenticated. Once reforms are complete, Open Banking obligations may arise from four sources: the PSRs, FCA rules under DUAA, Future Entity standards and commercial scheme rulebooks. Their cumulative burden, especially on smaller ASPSPs, should be assessed as a whole.

Q27: Are there any other adjustments needed to current regulation which would better support Open Banking?

Members made three points. First, as above, the framework should be consolidated so that firms can see in one place where every Open Banking obligation sits. Second, the slow adoption of Open Banking payments reflects a commercial model that has not worked; the reforms under Questions 22 and 34 should be judged by whether they fix that. Third, warnings and confirmation steps added to Open Banking journeys have created friction that is holding back adoption. Friction should be proportionate to risk. In addition, we would support: equal treatment of banks and non-banks seeking account information and payment initiation permissions (Question 9); raising the prohibition on ASPSPs creating obstacles to third-party access into legislation, with specific obstacles addressed in FCA rules; and a proportionate exemption from the obligation to maintain a dedicated interface for ASPSPs that can show no third-party demand, as the EU has adopted. Open Banking reforms should also be coordinated with the Retail Payments Infrastructure Board's work.

Providing the FCA with powers to regulate Open Banking under the Data (Use and Access) Act 2025

Q28: Do you agree with the proposed approach to provide the FCA with powers to place interface-related requirements on ASPSPs, PISPs and AISPs?

Yes, with two conditions. First, the FCA should publish a standards roadmap so that firms can plan build cycles, rather than react to individual rule changes. Second, the powers must be used. Members recalled that a year after Open Banking went live some firms still lacked developer portals, with no public regulatory action. Powers that are held but not exercised do not improve API quality.

The power to decide which firms fund the Future Entity is the one most likely to affect smaller firms on both sides of the market, and should not be delegated without constraint. The instrument should require a proportionate funding formula, with a floor below which firms contribute nothing or a nominal amount, tapering by size or volume, no double contribution by firms active on both sides of the market, and consultation before any determination or material change.

Q29: What are your views on whether the FCA should be provided with a power to mandate ASPSP participation in commercial Open Banking schemes?

We note that the Government does not propose this power, relying instead on the new right of access for variable recurring payments and fair commercial arrangements to encourage participation. Members' views differ. Some ASPSP members agree that participation should not be mandated. Third party providers are concerned that, without a mandate, account coverage for commercial schemes may remain incomplete. We suggest a way to reconcile these views. HM Treasury should not take the power now, but should commit to a review at a defined point, for example two years after the new right of access commences, against published measures such as account coverage of the commercial variable recurring payments scheme and the range of use cases live. If coverage falls short, HM Treasury should then consult on a targeted power, limited to the scheme concerned and falling away once coverage is achieved. Whether or not participation is ever mandated, scheme governance should give PISPs, AISPs and merchants a genuine voice alongside ASPSPs. Without that, schemes would move today's disputes about API quality into a body with more formal power and the same incentives.

Q30: Would it be beneficial to maintain a requirement on ASPSPs to publish 'product' and 'reference' information via Open Banking APIs, as is required today under the CMA Order?

Members did not raise specific evidence on this question. On balance, we see value in maintaining the requirement while the FCA assesses how the data is used, because removing an established data flow is harder to reverse than keeping it. We would support a review based on usage evidence.

Q31: Would it be beneficial to maintain a requirement on ASPSPs to enable sweeping variable recurring payments? If so, what should the scope of application be?

Yes. Sweeping is the use case with the clearest consumer benefit and has been the proving ground for commercial variable recurring payments; the requirement should be maintained and should remain free of charge, with that principle set in legislation. The ASPSPs currently covered by the CMA Order should remain in scope. If scope is widened, it should be on the same demand-based test we propose under Question 21, so that ASPSPs, including payment

and e-money institutions, whose customers see no third-party demand are not required to build capability that will not be used.

Q32: Do you agree with the proposed approach to providing the FCA with powers to regulate the Future Entity as an interface body?

Yes. Regulation of the Future Entity should preserve its operational independence from any single participant group, and give it enough authority, backed by the FCA's supervisory and enforcement tools, to resolve API performance disputes in practice.

Q33: Do you consider there would be any competition law barriers to the operation of commercial Open Banking schemes under the proposed approach and, if so, how might these be addressed?

Members did not identify specific barriers in our session. The obvious risk area is collective price setting within schemes. There is already a live example of the approach we favour. The FCA and the Payment Systems Regulator have stated that they will not, at this time, prioritise investigation under Chapter I of the Competition Act 1998 of UKPI's pricing arrangements for commercial variable recurring payments, subject to safeguards embedded in UKPI's governance, and the CMA confirmed in January 2026 that it does not intend to take a different position. That comfort is, however, limited to the first wave of use cases and lasts only until the DUAA regime is implemented or July 2027, whichever is earlier. Scheme design should be tested against competition law before schemes are established, for example through joint FCA and CMA guidance or a standing mechanism, building on the UKPI precedent, giving comfort on scheme rules in advance, rather than risks being discovered through later intervention.

Q34: Do you agree that the FCA should have powers to intervene directly in the pricing of Open Banking access arrangements where necessary? Should those powers differ depending on whether the pricing arrangement is established through a commercial scheme or outside a commercial scheme? Please explain your answer.

On balance, yes, as a backstop. Open Banking payments have not been adopted as quickly as they should have been because the commercial model has not worked. Whether that amounts to a market failure is debatable, but something needs to change, and our members would support these powers unless there is good reason not to. The powers should be a backstop for demonstrated market failure, not a default price-setting function, since routine intervention could deter commercial schemes from forming.

The powers should differ. Where pricing is set within a commercial scheme with balanced governance and published terms, the FCA should intervene only exceptionally. Where pricing is set bilaterally outside a scheme, a stronger backstop is justified, because the protection that scheme governance provides is absent.

Q35: Do you agree with the proposed approach to providing the FCA with powers to regulate commercial Open Banking schemes?

Yes. The powers should distinguish between scheme rulebooks, covering standards, liability and dispute resolution, and commercial terms, and be proportionate to each. Regulation should support schemes forming, not discourage them.

Q36: Are there additional powers in relation to participating firms (ASPSPs, PISPs and AISP), the Future Entity or commercial schemes that the FCA might need to effectively manage Open Banking into the future?

Members' concern is less about new powers than about the use of existing ones. The FCA's wider supervisory toolkit, including voluntary and imposed requirements and skilled person reviews, has a lower threshold than formal enforcement and can be more effective in resolving API performance problems. The FCA should also have the ability to impose financial penalties where interface requirements are persistently breached. What matters is that the tools are used.

FCA monitoring and enforcement powers

Q37: Do you agree with the proposed approach of mirroring as closely as possible the FCA's monitoring and enforcement powers as set out in FSMA?

Yes. Mirroring the FSMA toolkit gives firms familiar processes and safeguards, including rights of representation and reference to the Upper Tribunal, and is proportionate.

Q38: Do you have views on the FCA being given a power to issue compliance notices to enforce compliance with requirements made under DUAA?

We support it as a graduated tool that sits below full FSMA enforcement in severity and process. The CMA already has comparable powers in relation to Open Banking, and it is sensible for the FCA to hold them as the CMA's role ends. The process should include notice, an opportunity to respond and a reasonable period to remedy, with published criteria for when notices will be used.

Q39: Do you envisage scenarios where it would be helpful for the FCA to share certain confidential information with the Future Entity, in connection with the FCA's role as regulator for Open Banking?

Yes, in limited cases, for example, sharing interface performance data, coordinating responses to incidents and outages, and sharing information on fraud patterns affecting Open Banking payments. Sharing should be tightly scoped to the Future Entity's functions, with confidentiality protections equivalent to the FCA's existing information gateways. Sharing must be strictly controlled so that competitively sensitive information is not shared, particularly as the Future Entity's board may include representatives of competing firms.

Q40: Do you agree with mirroring the FCA's FSMA objectives and matters to which it must have regard for the purpose of the FCA exercising its new powers and functions in relation to Open Banking?

Yes. This provides consistency, and should include the FCA's secondary objective on international competitiveness and growth.

Q41: What are your views on providing the FCA with an additional objective which reflects the broader data-focused aims of DUAA to support its approach to regulating Open Banking?

Members do not support an additional objective. Innovation is best delivered by industry, and the FCA's existing competition objective and its secondary objective on competitiveness and growth already give it the necessary mandate, and regulators should focus on clear, proportionate guardrails that enable market-led innovation. A new objective risks being a

statement of intent that changes no regulatory decision. A more useful step would be for the FCA to report regularly against measurable Open Banking outcomes, such as adoption, API performance and the range of services available.

Q42: Are there any other areas of feedback on issues raised in this consultation?

We would highlight five points:

- **Coordination.** These reforms must be joined up with the Retail Payments Infrastructure Board's work, the National Payments Vision, the systemic stablecoin regime and the consolidation of the Payment Systems Regulator into the FCA. Our responses to those consultations make the same point from the other direction.
- **Sequencing.** Items that do not depend on the full rewrite, in particular recognised jurisdiction decisions and the remaining custody barrier for stablecoin payment acceptance, should, in the view of most members, be taken forward now. Some bank members disagree.
- **Transition.** Timelines should be clear and realistic, existing permissions should carry across automatically, and firms should not have to rebuild systems twice.
- **Capacity.** The FCA's resources should match its expanding responsibilities.
- **Clarity.** Firms need a formal, timely route to clarification on FCA rules, and new expectations should be set out in published rules rather than introduced through thematic reviews.

Conclusion: five recommendations to HM Treasury

Drawing together the answers above, if TPA were to make only five recommendations to HM Treasury, they would be:

1. Keep legal certainty where it matters, and put guardrails on delegation: keep the perimeter, core user rights, core safeguarding and the principle of authentication in statute, and keep payment firms outside Part 4A of FSMA; move operational detail to FCA rules through a policy-neutral transfer, with proper cost-benefit analysis for later changes, a formal route to clarification and a single consolidated guide; replace prudential requirements set bilaterally through supervision with published, proportionate standards; and strengthen payment firms' access to bank accounts and to safeguarding at the Bank of England.

2. Fix today's tokenised payment barriers now, not in 2028 (a majority view; some bank members disagree): publish the recognised jurisdiction criteria and decide on the EU and US regimes quickly; widen the exclusion so that payment firms holding stablecoins for customers do not need a cryptoasset safeguarding permission before stablecoin safeguarding moves into the payments regime; and extend streamlined payment permissions to authorised wallet and custody providers, not only issuers.

3. Regulate by activity and risk, not technology: use one set of regulated activities for tokenised and conventional payments, avoid variations of permission based on technology alone, and take the opportunity to redesign the perimeter from first principles so that firms know what requires permission and which permission applies.

4. Make agentic payments accountable by design: recognise mandate-based consent with clear scope, limits and revocation; allocate liability by role across the chain, including technology providers closely involved in instructing or triggering payments; and protect vulnerable customers without adding friction that deters adoption.

5. Give Open Banking a sustainable commercial model backed by enforceable standards: keep baseline access under regulations 69 and 70 free and contract-free; allow charging for services beyond that baseline in return for mandated, monitored and enforced API standards; consolidate the framework into one clear statement; and give the FCA powers it will use as backstops, without an additional innovation objective.

TPA and its members stand ready to support HM Treasury and the FCA as this work progresses, including through our working groups. We would welcome the opportunity to discuss any of the points raised in this response in more detail.

About The Payments Association

The Payments Association is for payments institutions, big and small. We help our members navigate a complex regulatory environment and facilitate profitable business partnerships.

Our purpose is to empower the most influential community in payments, where the connections, collaboration and learning shape an industry that works for all.

We operate as an independent representative for the industry and its interests, and drive collaboration within the payments sector to bring about meaningful change and innovation. We work closely with industry stakeholders such as the Bank of England, the FCA/PSR, HM Treasury, Pay.UK, UK Finance and Innovate Finance.

Through our comprehensive programme of activities for members and with guidance from an independent Advisory Board of leading payments CEOs, we facilitate the connections and build the bridges that join the ecosystem together and make it stronger.

These activities include a programme of digital and face-to-face events including our annual PAY360 and FC360 conferences, our PAY360 Awards dinner, PA@The City, CEO round tables, webinars, working group events and training activities.

We run focused stakeholder working groups spanning Agentic Commerce, Cross-Border, Digital Currencies, ESG, Financial Crime, Financial Inclusion, Merchant Payments, Open Banking, Regulatory, and Payments Infrastructure. The volunteers within these groups represent the collective view of The Payments Association members at industry-critical moments and work together to drive innovation in these areas.

Our Payments Intelligence team and our working groups aim to produce regular thought leadership for our membership and beyond. These include data-driven reports, articles, video interviews and podcasts. We also undertake policy development and government relations activities aiming at informing and influencing important stakeholders to enable a prosperous, impactful and secure payments ecosystem.

See www.thepaymentsassociation.org for more information.

Contact natasha.healy@thepaymentsassociation.org for assistance.