



connecting the future

RPIB Consultation
on the Design of the Future Retail Payments
Infrastructure

Bank of England
on behalf of the Retail Payments Infrastructure Board
25 June 2026

Response from
The Payments Association

Introduction

The Payments Association (“TPA”) welcomes the opportunity to respond to the Retail Payments Infrastructure Board’s (RPIB) consultation on the design of the future retail payments infrastructure, published by the Bank of England on 25 June 2026. Our members consider this the most important payments initiative in a decade and have engaged with urgency and depth.

This response reflects views expressed by TPA members and industry experts who contributed through a dedicated members' workshop and follow-up written submissions. As TPA's membership spans the full payments value chain (banks, non-bank PSPs, card schemes, fintechs and their advisers) and holds a correspondingly diverse range of views, this response cannot and does not claim to represent the position of every member on every question.

We are grateful to the contributors to this response, which has been drafted by Robert Courtneidge on behalf of TPA's Policy team. We would also like to thank the Bank of England and the RPIB for their continuing engagement with industry throughout this process. We hope this response supports the shared goal of ensuring the UK's next-generation payments infrastructure keeps the UK the best place in the world for payments businesses to establish, invest and grow.

Emma Banymandhub

CEO

The Payments Association

Executive summary:

The Payments Association's five tests for the future infrastructure

Before drafting detailed responses to each consultation question, The Payments Association (TPA) convened a members' workshop to test the RPIB's proposals against five criteria. These tests frame our detailed answers below and underpin the recommendations in our conclusion.

1. Future-proof: design for unknown use cases, not just today's payment rails.
2. Open & competitive: access and standards should enable fintechs, PSPs and new entrants to compete.
3. Right-sized core: keep only essential clearing/messaging functions in the core; avoid crowding out competitive services.
4. Interoperable: support different schemes, providers and forms of money through common standards and interfaces.
5. Safe & viable: embed resilience and appropriate fraud capabilities while ensuring adoption and migration are economically viable.

These tests inform five recommendations we ask the RPIB to consider in finalising its design, set out in full in our conclusion: future-proof the core; protect competition; keep the core focused; make interoperability real; and deliver safely and economically.

General observations

TPA members broadly endorse the direction of the RPIB's proposals, particularly their emphasis on future-proofing, interoperability, competition and avoiding unnecessary expansion of the core infrastructure. The workshop identified several cross-cutting themes that extend beyond individual consultation questions, and which we encourage the RPIB to consider throughout the design process.

1. Governance is as important as technology. The long-term success of any future infrastructure will depend on standards and rules developed and administered through collaborative governance by non-bank PSPs, fintechs, merchants and other users, alongside traditional banking participants. Expertise from all parties should define the standards against which services are delivered.
2. Access requirements should be proportionate to market significance, built on capability, risk management and regulatory status rather than institutional type. Open and competitive outcomes will be difficult to achieve if participation remains overly dependent on existing rules and processes.
3. Delivery Company funding and governance must be resolved early and transparently. Lessons from prior UK payments infrastructure initiatives point to the risk of ambitions being diluted where funding is uncertain. A robust roadmap, with milestones based on delivery of benefits and with continuous oversight of cost and delivery, should be considered from the outset.

4. We are concerned that the consultation sets out no indicative timeline for phases 2 to 4 of delivery, and defers questions of cost and funding for principles, such as security, scalability and resilience, that will require substantial technology investment to achieve. We ask the RPIB to address both gaps before, or alongside, finalising its design, so members can plan investment and resourcing with confidence. We recognise that phases 2 to 4 might realistically be iterative, and this should also be reflected in the next iteration of the plan.
5. Engagement with this consultation has been exceptionally strong: more than 30 TPA members registered for workshop sessions, with 40–50 participants expected across working group discussions, and members have offered to support further follow-on discussions and working groups as the response develops. We see this as a clear signal of the industry's readiness to help shape, fund and adopt the future infrastructure, and would welcome continued close dialogue with the RPIB as the design develops.

Our members' views:

We respond to this consultation question by question, following the structure of the RPIB's consultation paper.

Question 1: Are the end-user payment journeys presented sufficient to inform the design of the core infrastructure?

a. Are there any additional or alternative payment journeys that should inform the design of the core infrastructure? If so, please specify what these are.

b. Are any of the payment journeys not appropriate as inputs to the design of the core infrastructure? If so, please specify what these are.

Members consider the journey set a good starting point but not yet sufficient. The set should be deliberately forward-looking and cover consumer, SME, corporate, government, cross-border and embedded payment needs, expressed as outcomes and capabilities rather than tied to a particular technology, so that the design would still work even if the dominant payment proposition of 2035 cannot be named today.

One specific gap: the journeys as presented focus on 'straight-through' processing. In practice, much of the cost and customer frustration in payments arises from exception handling – accounts closed, blocked or suspended, chargebacks, insufficient funds and similar scenarios. We recommend that these exception journeys are recognised in the core requirements from the outset, rather than treated as an add-on once the primary journeys are built.

Members also noted that cash and ATM/LINK journeys should be explicitly included within the payment journey set: cash remains the primary means of payment for millions of consumers, and the Bank's own definition of 'interoperability' extends to interoperability with cash. We understand LINK's own consultation response will call for payment journeys involving cash to be explicitly considered as part of the core design work, including through an engagement forum on core payment journeys, and for exploration of contactless-enabled ATM terminals to support this interoperability; we would support the RPIB taking this forward (see also our answer to Question 11).

Question 2: Do you have any views on the key considerations that should guide migration timelines and product roadmaps for delivering the PVDC's outcomes?

Migration timelines and product roadmaps should be driven by the practical dependencies, risk controls and regulatory alignment needed to deliver the PVDC's outcomes safely and efficiently.

Infrastructure dependencies and legacy constraints

Roadmaps should take account of contractual end dates, renewal cycles and legacy service constraints, to minimise disruption, avoid unnecessary investment in services that may soon be replaced, and prioritise areas where current platforms constrain innovation, efficiency or richer data capabilities.

Risk management

A phased migration approach should reduce operational and systemic risk. Initial phases should focus on establishing overall programme governance and capabilities to enable safe

migration from the existing legacy infrastructure, establishing the core infrastructure, onboarding participants, and supporting new products and services before migrating established payment schemes. This would allow the platform to demonstrate resilience and operational maturity while giving participants experience of integration, testing and operational processes. Lower-risk services could then be migrated incrementally before systemically important, high-volume services such as Faster Payments and Bacs are transitioned, with managed coexistence between incumbent and new platforms where needed to support market readiness, customer transition and contingency planning.

Members also stressed the importance of a credible, practical migration path for specific high-volume legacy journeys, Direct Debits and wider Bacs functionality, not only the target-state design: success will be measured as much by how confidently these journeys move onto the new infrastructure as by the design itself.

Regulatory alignment and avoiding duplicate investment

Migration planning should be closely aligned with the wider UK financial services regulatory agenda, including Operational Resilience, Consumer Duty, Critical Third-Party requirements, fraud prevention initiatives, Open Banking developments and ISO 20022 adoption. Coordination between regulatory change and next-generation infrastructure implementation is essential to avoid a 'build twice' scenario, particularly for capabilities that depend on payment data, message structures, workflow integration and control points, such as fraud controls, Confirmation of Payee enhancements, regulatory reporting, transaction monitoring, sanctions screening and digital identity services.

Industry confidence will also depend on clarity around migration costs, coexistence arrangements, testing, resilience expectations and the treatment of existing investment.

We would also ask the RPIB to publish a roadmap that emphasises iterative delivery rather than a single end state. World-leading account-to-account systems have continued to develop well beyond their initial launch, and the next stage of this work should show how the infrastructure will keep evolving after the initial build and migration, not only how it will be delivered once.

As set out in our general observations above, we ask the RPIB to publish indicative dates for phases 2 to 4 of delivery as a priority, given the resourcing decisions members must make in the meantime.

Question 3: Do you agree with the list of proposed design principles?

a. Are there any additional design principles that should be included? If so, please specify and explain.

b. Are there any alternative design principles that should be included? If so, please specify and explain.

We broadly agree with the proposed design principles, which provide a strong foundation for the future payments ecosystem. However, given the systemic importance of UK payments infrastructure, some of our members recommend sovereignty is included as an additional design principle.

Payments infrastructure is critical national infrastructure, and we see this less as a standalone design principle than as a resilience and dependency-management question that should sit alongside the RPIB's existing governance and resilience thinking. The next-generation infrastructure should be able to preserve continuity of critical functions

(auditability, recoverability and the ability to respond under UK governance) without excluding international technology providers or slowing innovation. This connects to a related strand of government work: the Department for Business and Trade's Call for input on potential powers to protect the UK from adverse economic pressure (published 9 April 2026, closed 18 June 2026) considered the concentration of UK payment volumes with a small number of non-UK-domiciled providers, and the practical difficulty of using any new government powers if the underlying rails cannot themselves withstand disruption or withdrawal by those providers. A TPA representative attended DBT's roundtable on this call for input, held on 18 May 2026 alongside TheCityUK, UK Finance, Innovate Finance and several major banks, where these concentration and resilience concerns were raised directly with officials; we cross-refer to it here because the RPIB's decisions on resilience and dependency management bear directly on it, even though our members are not agreed that this should become a distinct, named design principle. Considerations members raised under this heading included:

1. Maintaining data sovereignty: UK control over the storage, processing, access and administration of critical payment data, including during support, maintenance, incident response and disaster recovery.
2. Maintaining operational sovereignty: ensuring critical operational functions can be performed, supervised and recovered by UK-based entities.
3. Managing technology and infrastructure dependencies: identifying and actively managing reliance on non-UK technology providers (software, hardware, cloud, support and maintenance) and preventing critical operational control from depending on non-UK entities or jurisdictions.
4. Preserving jurisdictional control: ensuring governance, oversight, dispute resolution and decision-making remain subject to UK regulatory, supervisory and national interests.
5. Strengthening supply-chain resilience: mitigating risks associated with software updates, security patches, hardware availability, support models and third-party concentration.

We recognise this is a live and, among our own members, contested question: some feel these concerns are better addressed through the RPIB's existing resilience and governance principles than through a new, separately named 'sovereignty' principle, and are concerned that framing it as a standalone principle could be read as favouring UK-based providers over global capability, competition and innovation. We raise it here, rather than setting it aside, because of its relevance to the DBT work referenced above, and would welcome the RPIB's own assessment of how far resilience against concentration and dependency risk is already captured elsewhere in its design principles.

We would also make modularity, extensibility and technology neutrality explicit design requirements, and ensure 'open access' is meaningful, risk-based and proportionate rather than restricted to incumbent business models.

Question 4: Are there any design principles which you would prioritise over others? If so, please explain why.

a. What are the key trade-offs to consider, and what are their implications for design choices (for example, in relation to performance, scalability, and cost)?

Members were clear that adaptability should be prioritised over any fixed view of today's end-user propositions. Designing for unknown user behaviour five to ten years ahead is genuinely difficult; the safer design choice is a core that enables quick innovation at higher layers, rather than one that locks in specific products or features. This represents a deliberate shift away from prior UK payments infrastructure efforts, which in places focused

too heavily on current end-user features baked into the core (for example BACS) at the expense of long-term adaptability.

The key trade-offs the RPIB will need to navigate, in our members' view, are: standardisation versus innovation; resilience versus speed of change; open access versus risk controls; and future-proofing versus cost and complexity. We would ask the RPIB to state explicitly, principle by principle, where it expects to sit on each of these trade-offs, so that the design principles constrain future decisions.

Question 5: Do you agree with the proposed conceptual architecture? If not, please explain why and what changes you would propose.

We support a 'thin core' model: a core infrastructure that provides the minimum set of common capabilities required to deliver safe, efficient and interoperable clearing and messaging for all fast payment volumes and account-to-account transactions, with competitive services kept outside the core unless there is a compelling market-failure or interoperability case for including them.

This is consistent with the strong member support we have heard for avoiding unnecessary expansion of the core infrastructure: the architecture should permit multiple schemes, products and services to innovate on top of common infrastructure, rather than the core itself competing with the market it is meant to serve.

Members also stressed that governance of the services around the core (identity, payment authorities, fraud services, and Confirmation of Payee-type capabilities) matters as much as governance of the core itself. These should sit outside the core, but responsibility for them must not become fragmented or duplicated across too many bodies, or the benefits of a thin core will be undermined by an incoherent periphery.

The open question our members raised is governance: who decides where the boundary between core and competitive ecosystem sits today, and what governance process exists to revisit that boundary as the market evolves? We ask the RPIB to set this out explicitly, given how consequential the boundary decision will be for competition and innovation over time.

Question 6: Does the architecture draw boundaries between the layers appropriately? If not, please explain why and what changes you would propose.

Broadly, yes, subject to two qualifications. First, interoperability should be embedded in the design from the outset, rather than addressed later as an integration layer (see our response to Question 11 below). Secondly, common services, including identity and credentials, data, and programmability, should be assessed on a case-by-case basis: they should be common where technically or economically necessary, and left to competitive provision where that is appropriate.

As decisions are taken on the boundary between the core and the wider ecosystem, we would encourage the RPIB to assess the impact not only on resilience and efficiency, but also on innovation, competition, new entrants and consumer choice.

Members were also clear that certain industry services, such as alias databases and Confirmation of Payee, should be designed and delivered alongside the core as shared industry utilities, rather than developed separately by each participant; delivery through a single entity would support consistency and operational efficiency, and would align with wider Bank of England initiatives in this area. Other members took a different view: rather than centralising delivery in a single entity, these services, including analytics, should be

designed and delivered with reference to commonly developed standards (for example for message and/or API content), with delivery itself open to competition between providers, since this would better support innovation and efficiency while still delivering consistency.

Question 7: What are the baseline services that should be delivered within the core infrastructure? Please include an explanation of why.

The baseline should cover only clearing, settlement and messaging for fast payments and account-to-account transactions. It should also include the shared industry utilities noted above, such as analytics, alias databases and Confirmation of Payee. These services are best provided through a common layer. Duplicating them across providers would be inefficient. A trusted shared service would also help reduce fraud and improve interoperability. We also ask the RPIB to consider whether the role of open banking services should be included in the baseline. These could include account information and push payment initiation. As payments rely more on data, there may be scope to combine data and transaction services in a more joined-up way.

Question 8: What payment-enabling or value-add services should be delivered separately from the core? Please include an explanation of why.

In our members' view, orchestration and digital asset capabilities should sit outside the core. They should ideally be delivered before, or at the same time as, the wider infrastructure build. An access and orchestration layer is, in our view, essential to enable participants to migrate from legacy arrangements to the new infrastructure more easily. This layer should include good APIs, automated onboarding, software development kits, reference examples and sandbox testing. These tools should be maintained throughout the life of the infrastructure. This approach would help participants of all sizes and bring useful capability to market faster than waiting for the full core to be delivered. Given appropriate standards, this layer could be provided to participants as an extension to existing technical service providers' offerings (for example, gateways) on a competitive basis.

More generally, value-added services should be assessed individually. They should remain outside the core unless there is a clear reason to centralise them. That reason should be based on market failure or the need for interoperability. This is consistent with our answer to Question 6.

Question 9: What opportunities and challenges could digital identity frameworks and the use of credentials (e.g. Legal Entity Identifiers or other verifiable credentials) present in enhancing retail payment journeys?

Digital identity and credential frameworks could reduce friction and fraud in retail payments. For example, they could reduce repeated identity checks across providers. They could also support clearer and more reliable consent for delegated and agentic payments, as noted in our answer to Question 17. The main challenge is design risk. These capabilities must not create a single point of failure or lead to unnecessary centralisation. Access should also be open and not depend on a small number of existing identity providers. In addition, such capabilities should not be developed in a 'retail payments stovepipe': retail payments should rely on cross-sector digital identity frameworks and assets.

Digital identity and credential capabilities within the future retail payments infrastructure should not be developed in isolation from the significant cross-economy and sector-specific work already under way. At a national level, the RPIB should engage with the Office for Digital Identities and Attributes, within the Department for Business, Innovation, Science and Technology. OfDIA maintains the statutory UK Digital Identity and Attributes Trust

Framework, which establishes rules and certification arrangements for trusted digital verification services and supports the secure reuse of identities and attributes across the economy. HM Treasury and DBIST have also published guidance clarifying how certified digital verification services may be used for customer due diligence under the Money Laundering Regulations. Importantly, digital verification can support these checks but does not replace the legal and regulatory responsibilities of the relevant regulated firm. For high-value property payment journeys, the RPIB should also engage with the Digital Property Market Steering Group, which is chaired by the Ministry of Housing, Communities and Local Government and brings together government, regulators and industry to support a more digital and data-enabled property market. Its current work includes reusable digital verification, Qualified Electronic Signatures and the alignment of identity verification with the wider home-buying and selling process. HM Land Registry should also be included: it maintains a Digital Identity Standard for parties to registrable property transactions, while recognising that separate AML and professional obligations continue to apply. The Open Property Data Association is a further important industry partner: OPDA has developed common property data standards and is closely involved in work on the Smart Property Data Trust Framework, addressing trusted data, provenance, participant credentials, permissions, consent and interoperable APIs across the property transaction. We therefore encourage the RPIB to engage with OfDIA, HM Treasury, DPMSG, HM Land Registry and OPDA so that identity, authority and credential capabilities within payments are interoperable with existing national and sector frameworks, avoid duplicating work already under way, and preserve clear responsibility for AML, fraud prevention and reliance on verified information.

Question 10: Are there other cross-cutting, architecture-wide issues that should be considered to meet the PVDC outcomes, that go beyond the core infrastructure layer? If yes, please explain.

Yes. Four cross-cutting issues stood out in our members' discussions.

1. Regulatory fragmentation.
Members noted overlapping and, at times, inconsistent requirements across the PSRs, the CMA9 arrangements, FCA technical standards and data legislation; a clear, consolidated regulatory framework for payments and data would materially help. Members also observed that major innovations, stablecoins and agentic commerce among them, are being regulated in silos by different regulators, and that a coordinated regulatory and industry response is needed to avoid fragmented growth as the future infrastructure comes online.
2. Terminology and document alignment.
This consultation and the RPIB's related 'Roles and Responsibilities' policy paper use different terms for related concepts, which complicates a coherent industry response. We ask the RPIB to publish a single, consistent glossary across its published and forthcoming documents.
3. Transaction transparency.
Payment process data should be made available to ecosystem participants in a structured way, so that a payment does not simply disappear into a black box once initiated. We recognise there are fraud and compliance considerations to manage carefully here, but see this as an opportunity to build transparency, and a foundation for new products and services, into the design from the outset via a generalised, open approach to enriched transaction data.
4. Ecosystem coordination.

We are concerned that the consultation does not yet sufficiently address how the core layer will coordinate with settlement infrastructure and other ecosystem participants. We would welcome further detail on this in the next stage of the RPIB's work.

Schemes and standards governance. The consultation does not yet address how the schemes and standards that sit around the core should work together. Without a joined-up approach spanning new forms of money (including systemic stablecoins, tokenised assets and CBDC), new account-to-account and open banking arrangements, and legacy schemes such as LINK, cheques and Bacs, there is a risk of a fragmented and costly landscape, with an unsustainable administrative burden for firms participating across multiple schemes. We would encourage a single, joined-up and sovereign approach to schemes and standards governance that is not-for-profit, open access and regulated.

Question 11: Do you agree with the proposed approach to interoperability? Please explain your reasoning.

We support the direction of travel, but would stress that interoperability is not solely a technical issue: connecting different schemes or forms of money is only part of the challenge. Commercial arrangements, settlement models, liability frameworks, dispute management and governance are likely to be just as important as common standards and interfaces in determining whether interoperability succeeds in practice. Open where possible, controlled where necessary, with clear rules, transparent pricing and effective industry governance, is the framing we would encourage the RPIB to adopt. Several members also felt that interoperability with existing, non-digital forms of payment, cash in particular, is currently under-addressed in the consultation's framing (see also our answer to Question 1).

Question 12: What are the potential trade-offs between different settlement models in terms of speed, payments certainty, liquidity management for participants, operational complexity, and scalability?

Settlement arrangements need to support resilience, liquidity efficiency and the multi-money ecosystem the National Payments Vision envisages, rather than being optimised solely for the account-to-account journeys that exist today. We would encourage the RPIB to test candidate settlement models explicitly against the ability to accommodate bank money, e-money and emerging regulated digital forms of money, including regulated stablecoins, without requiring repeated redesign of the core each time a new form of money is added; in our members' view, this risk of repeated redesign, more than the challenge of supporting any single new form of money, is the key design challenge here.

Question 13: What additional design, governance and operational issues would need to be addressed to achieve interoperability?

Access is the main operational issue. Strong APIs, automated onboarding, software development kits, reference examples and sandbox testing are needed for interoperability. They are not optional extras. These tools should be maintained throughout the life of the infrastructure. They should support new participants, as well as testing and development by existing participants. We also support access criteria that are clear and proportionate. These criteria should support both indirect and direct participation. Governance should also give fintechs, PSPs, merchants and other users a meaningful voice in standards and rules, alongside established banking participants.

Question 14: Do the architecture and core infrastructure design choices outlined in this consultation capture the key considerations necessary to support account-to-

account payments at PoS, both online and in-store? If no, please specify and explain why.

a. Are there additional opportunities or challenges that should be taken into account? If yes, please describe them and explain why.

The architecture and core infrastructure design choices do not yet fully address the requirements for account-to-account payments at the point of sale. These payments need instant payment confirmation. Merchants also need real-time messages that confirm funds will be available for settlement. Current systems do not provide this consistently. The next-generation infrastructure should address this gap directly. It should not assume that faster clearing will solve it.

More broadly, infrastructure alone will not make account-to-account payments at the point of sale commercially viable, a point we would emphasise strongly. Clear scheme rules will also be needed, sitting outside the rulebook for core interbank infrastructure. Commercial incentives and consumer protections will also be important: account-to-account payments at the point of sale do not need to replicate cards, but they do need a clear value proposition, appropriate customer outcomes, sustainable commercial incentives and supporting governance, with consumer protections comparable to those consumers already expect from cards. Together, these measures will help build trust among merchants and consumers.

Question 15: What are the key design considerations for the next-generation infrastructure that could help solve existing challenges with cross-border payments?

a. What are the most appropriate solutions to target?

The core standards and infrastructure, as developed, should be open to use as the first or final mile in cross-border transfers. Requirements for participants to support 'one-leg-out' (OLO) payments alongside purely domestic payments should be built into the core scheme and infrastructure, with appropriate data and other provision, rather than relying primarily on interlinking nationally separate real-time payment systems, which is complex and would take time. We encourage the RPIB to prioritise adoption of common standards to facilitate interoperability, alongside solutions such as One-Leg-Out capability. This would allow the UK to position itself as a natural hub for global payments. It should be treated as more than a domestic infrastructure upgrade.

Question 16: What functional requirements would next-generation infrastructure and the wider next generation ecosystem need to meet to enable programmable payments at scale, while maintaining resilience and user trust?

The infrastructure should enable programmable payments at scale while maintaining resilience and user trust. It should support a broad capability, rather than prescribe a single use case. In particular, it should support conditional and automated payment logic. It should also avoid building specific business models into the core. This would allow competing programmable payment services to develop on top of common infrastructure. It would also help the ecosystem adapt as new payment models emerge.

We also note a definition risk in the consultation. The distinction between programmable payments and advanced delegated payments may confuse the technology with the user journeys it supports. Programmability is a functional capability. Delegated payments and agentic payments are use cases that this capability can support. Those use cases may develop in different ways over time. We therefore recommend that the RPIB separate the capability from the use cases it enables. This would help avoid uncertainty about scope as

the design develops. It would also support clearer rules, more flexible implementation and better long-term adaptability.

Question 17: What capabilities or functions would the next-generation infrastructure need to support the safe provision of agentic payments?

a. What barriers to their development or adoption would need to be addressed?

For the infrastructure to support the safe provision of agentic payments, it will need capabilities that maintain trust, consent, control, accountability and traceability for transactions executed by delegated parties, including AI agents and other authorised delegates. At a minimum, this means the infrastructure should be capable of allowing participants to:

1. Verify approved agents, so that only authorised agents can initiate transactions.
2. Verify and identify agent identity, so agents are uniquely identifiable and their authority verifiable.
3. Issue agentic payment tokens (i.e. payment credentials tokenised specifically for delegated or AI-initiated transactions).
4. Manage delegated authority, consent and intent to ensure consent is explicit, authenticated, verifiable and revocable, and supports user-defined controls such as transaction limits, merchant restrictions, spending categories and validity periods.
5. Maintain end-to-end traceability and attribution, to support dispute resolution, auditability, liability management, fraud investigation and regulatory compliance.

These same capabilities would also support advanced delegated payments where the delegate is a trusted person, such as a carer or family member, rather than an AI agent; we agree with the consultation's framing of agentic payments as an extension of advanced delegated payments, provided the distinction between the underlying technology and the specific use cases is kept clear.

On barriers to adoption, the technology barriers are, in our assessment, relatively low. Many underlying capabilities already exist within current payment ecosystems, tokenised payment credentials, delegated authority, consent management, transaction controls and auditability; and international card schemes, digital wallets and Open Banking-based services already allow users to authorise third parties, apply spending constraints, revoke permissions and maintain auditable records. The real challenge is creating a trusted, interoperable framework that applies these capabilities consistently to AI agents and other delegated actors, underpinned by clear governance, liability models, operational standards and trust frameworks.

The principal barrier to adoption of any RPIB-delivered agentic payment capability is more likely to be market timing than technology: by the time the future infrastructure introduces equivalent capabilities, commercial payment networks and platforms may already have established significant market share and consumer trust in this space. A sovereign capability nonetheless remains valuable for market diversity and healthy competition, provided it is interoperable with, and competitive against, existing solutions rather than a parallel, closed system.

This is closely aligned with TPA's own Agentic Commerce Working Group, launching in October 2026, which is developing industry recommendations on consent, authentication,

liability and agent identity for agentic payments, with the ambition of the UK being the first country with clear rules in this area. We would welcome the opportunity to invite the RPIB representatives to attend, input, and observe from time to time.

Finally, we note that a framework which, in places, still mirrors a 2017 model may struggle to keep pace with the rate of change in this area; we would encourage the RPIB to build formal, periodic review of the agentic and programmable payments provisions into its governance from the outset, rather than treating the initial design as fixed.

Question 18: Which consumer protection and fraud-related capabilities should be prioritised for inclusion in the core infrastructure, and why?

Infrastructure-level capabilities should focus on shared problems where common data, signals or controls materially improve outcomes across the ecosystem – for example, shared fraud signals and Confirmation of Payee-type services referenced in our answer to Question 6. We would caution against embedding detailed liability and reimbursement rules, or product-specific controls, in the core itself, since these rules need to be able to evolve faster than core infrastructure typically can; any mandatory capability should have a clear rationale, a measurable benefit and a proportionate implementation cost.

As set out in our answer to Question 1, we would also prioritise the design of exception-handling journeys (e.g. blocked or suspended accounts, chargebacks, insufficient funds and similar scenarios) as part of the core consumer protection and fraud capability, rather than as a later addition, since this is where much of the cost and customer frustration in the current system arises.

Resilience should also be designed across the ecosystem as a whole, including operational dependencies between the core and its participants and coexistence arrangements during migration, rather than being treated purely as a core-infrastructure design question.

Conclusion: five recommendations to the RPIB

Drawing together the answers above, if TPA were to make only five recommendations to the RPIB at this stage, they would be:

1. Future-proof the core: mandate modularity, extensibility, technology neutrality and capacity for unknown future use cases.
2. Protect competition: transparent, proportionate access and governance; preserve room for competing schemes, products and services.
3. Keep the core focused: include essential common infrastructure capabilities; avoid unnecessary vertical integration of competitive services.
4. Make interoperability real: common standards and interfaces across schemes, providers and forms of money, supported by workable commercial and liability arrangements.
5. Deliver safely and economically: proportionate fraud/resilience capabilities, clear migration milestones, sustainable funding and protection against barriers to adoption.

TPA and its members stand ready to support the RPIB's continued engagement with industry as this work progresses, including through further working group sessions, and 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 & 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 Agent 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 malik.smith@thepaymentsassociation.org for assistance.