

10 September 2026

Retail Payments Infrastructure Board
Bank of England
Threadneedle Street
London EC2R 8AH
Via the Bank of England consultation portal

Re: Consultation on the Design of the Future Retail Payments Infrastructure

Dear Members of the Retail Payments Infrastructure Board:

The Merchant Advisory Group (MAG) respectfully submits these comments in response to the Retail Payments Infrastructure Board's consultation on the Design of the Future Retail Payments Infrastructure. MAG appreciates the opportunity to comment on this important work.

MAG supports the Board's focus on end-user outcomes and the development of adaptable, resilient and competitive retail payments infrastructure. Merchants are end users of payment systems and invest directly in acceptance technology, checkout design, reconciliation, fraud controls, customer service and operational change. Their participation should therefore be continuous throughout design, delivery, migration and governance, rather than limited to one consultation.

I. Background

About the MAG. The MAG is a global organisation dedicated to driving positive change and innovation in the payments industry through merchant collaboration, education and advocacy. Representing over 200 of the world's leading merchants across many industries, including airlines, retail, restaurants, insurance, amusement parks, grocery and software, the MAG facilitates strategic engagement across North America, Europe and Asia. This response has been informed by discussion with MAG's European merchant advisers across retail, travel, hospitality, digital services, marketplaces and other high-volume payment environments.

This response reflects shared merchant priorities identified through discussion with MAG members operating across in-store, e-commerce, in-app, recurring and cross-border payment environments. It is intended to help ensure that the future infrastructure works reliably and affordably in real merchant environments and supports payment choice for customers.

II. MAG's Overarching Priorities

Design for real merchant journeys. The infrastructure should explicitly support one-time, recurring and variable recurring payments; in-store, e-commerce and in-app acceptance; outbound merchant and marketplace payouts; and associated refunds, reversals, exceptions and disputes.

Make payment certainty a baseline. A merchant must receive a near-instant, unambiguous and reliable success or failure status before releasing goods or services, supported by standard status messages, error codes and end-to-end traceability.

Ensure A2A is commercially viable. A2A at the point of sale will be more likely to scale where its all-in cost - including implementation, integration, operations, refunds and disputes - is transparent, predictable and supports a viable merchant proposition compared with existing payment methods.

Deliver consistent protections and customer experiences. Common minimum standards are needed for authentication, refunds, disputes, consumer protection, error handling and responsibility across banks, PSPs and payment products.

Manage migration costs and operational risk. Timelines should be readiness-led, tested across merchant verticals and channels, and designed to avoid unnecessary terminal replacement, certification work, fragmented integrations or prolonged dual-running.

Protect interoperability and payment sovereignty. The UK framework should align with relevant European and international standards so global merchants are not required to build duplicative national solutions, while retaining operational resilience and avoiding undue dependence on any single external provider or jurisdiction.

Give merchants an enduring role. MAG requests structured merchant representation in the RPIB, DeliveryCo and related working groups as detailed design, commercial arrangements and migration plans develop.

III. Responses to the Consultation Questions

Q1. Sufficiency of the proposed end-user journeys

The proposed journeys are a useful baseline, but they are not yet sufficient to capture the full range of merchant use cases that should inform the core design. In particular, the design should explicitly cover the complete lifecycle of commercial payments rather than treating initiation as the whole journey.

MAG recommends explicit recognition of one-time, recurring, scheduled and commercial variable recurring payments across physical, e-commerce and in-app channels. It should also cover outbound merchant and marketplace payouts to customers or sellers. The journey set should include refunds, partial refunds, reversals, cancellations, failed or timed-out payments, payout failures, exception handling and dispute resolution. These are everyday merchant and customer journeys and require common identifiers, status messages and traceability from initiation through reconciliation.

No proposed journey should be removed at this stage. However, emerging use cases such as deferred, programmable and agentic payments should be enabled through modular, extensible design rather than allowed to increase the cost, latency or complexity of today's high-volume payment journeys before demand and safeguards are established.

Q2. Migration timelines and product roadmaps

Migration should be staged, readiness-led and based on measurable end-user outcomes. The roadmap should publish clear dependencies, decision points and minimum readiness criteria before merchants or PSPs are expected to invest or migrate.

Any dual-running period should be long enough to protect continuity but time-limited and actively managed to avoid indefinite duplication of cost and complexity. Pilots should include merchants of different sizes and operating models, including high-volume, low-ticket, card-present, e-commerce, subscription, travel and cross-border businesses.

Before implementation dates are set, merchants need clarity on the product rulebook, liability, payment certainty, refund and dispute processes, error taxonomy, service levels, reporting, settlement and the commercial model. Migration planning must also assess changes to terminals, software, integrations and certifications. A centrally desirable change can create substantial distributed cost if merchant infrastructure and release cycles are not considered early.

The roadmap should also be coordinated with relevant European developments, including the progression of the digital euro and related payment and digital-identity initiatives. UK sequencing and standards should avoid requiring multinational merchants to undertake parallel, incompatible implementations or replace recently completed European work.

- Maintain existing payment choice and service quality until replacement products are demonstrably reliable and commercially viable.
- Use published conformance testing and operational readiness gates across banks, PSPs and acceptance providers.
- Provide sufficient notice and coordinated change windows so merchants can align investment, hardware and software release cycles.
- Measure conversion, latency, failure rates, false declines, reconciliation quality and total cost during pilots, not only technical throughput.

Q3. Proposed design principles

MAG agrees with the proposed principles of innovation and competition, open access, common utilities and standards, security and resilience, performance and scalability, and protection from fraud and wider financial crime.

The principles should be supplemented by four explicit end-user principles: payment certainty and operational transparency; commercial sustainability and proportionality; consistent, accessible user outcomes; and adaptability and international compatibility. These additions would keep design decisions anchored in whether a payment method can work reliably and affordably in real merchant environments. They should cover unambiguous transaction status, traceability, common error handling, transparent pricing and avoidance of unnecessary acceptance or migration costs.

Q4. Priority principles and design trade-offs

MAG would prioritise security and resilience, performance and scalability, common standards, and innovation and competition. These principles are mutually reinforcing. A payment option cannot create meaningful competition if it is slower, less reliable, less predictable or no cheaper to accept than established methods.

Trade-offs should be assessed from an end-to-end perspective. Feature richness must be balanced against latency, operational complexity and failure modes. Fraud controls must be effective without creating disproportionate friction or false declines, particularly for low-value and impulse purchases. Shared utilities may improve consistency and network effects, but their governance and pricing must not entrench a small group of providers. Resilience should not depend on merchants funding duplicative integrations or maintaining multiple inconsistent implementations.

- Speed versus control: preserve near-instant merchant confirmation while enabling risk checks to operate efficiently.
- Standardisation versus differentiation: standardise messages, status, key data fields, credentials and minimum protections, aligned with relevant European and international standards where practicable, while allowing competition in products and user interfaces.

- Core scope versus complexity: place systemic, universally required capabilities in the core and keep rapidly evolving product logic outside it, connected through common interfaces.
- Cost versus functionality: assess total ecosystem cost, including merchant development, certification, hardware, support and reconciliation, not only infrastructure build cost.

Q5. Proposed conceptual architecture

MAG broadly agrees with the layered conceptual architecture as a useful organising model. The model should nevertheless make the merchant acceptance function and the associated feedback loop more explicit. Merchants sit within the end-user and access layers, but design choices made in every other layer directly affect checkout conversion, cost, fraud, reconciliation, customer support and infrastructure investment.

The final architecture should therefore show how merchant requirements are gathered, tested and governed across layers. It should also prevent accountability from disappearing at layer boundaries. End-to-end ownership is essential where a payment fails, is delayed, is duplicated, must be refunded or becomes disputed.

Q6. Boundaries between architecture layers

The proposed boundaries are broadly reasonable as conceptual boundaries, but they should not become organisational silos. The design should define the interfaces, accountable owners, service levels, data hand-offs and escalation routes between layers.

In particular, the boundary between the core, services, schemes and product arrangements must not lead to fragmented transaction status, error codes, fraud controls or dispute outcomes. Common minimum requirements should apply end to end even where capabilities are delivered by different organisations. Merchant representation should be built into the governance and change processes for each layer that materially affects acceptance.

Q7. Baseline services within the core

The core should focus on the minimum systemic capabilities required to deliver safe, reliable and interoperable payments consistently across products. It should not prescribe merchant-facing commercial terms or funding arrangements that can be agreed between merchants and their payment providers, except where needed to protect end-to-end certainty or systemic integrity. MAG considers the following baseline capabilities essential.

- Clearing and settlement coordination, including clear rules for irrevocability and finality.
- High-performance routing, message validation and transaction lifecycle management for real-time and batch journeys.
- Near-instant, definitive and machine-readable payment status, including standard timestamps, identifiers and failure or exception codes.
- End-to-end traceability and auditable transaction references that support reconciliation, investigation, refunds and recovery.

- Standardised, secure interfaces and rich common messaging that avoid bespoke participant integrations.
- High availability, scalability, operational monitoring and tested fallback arrangements.
- Standardised data fields and control points needed for interoperable fraud and financial-crime prevention, including consistent payer and payee identifiers, relevant name fields, the initiation method, a mandatory agentic-payment flag and intent credential where applicable, and end-to-end references, subject to data-minimisation and privacy requirements.

Q8. Services delivered separately from the core

Rapidly evolving, competitive or user-facing capabilities should generally sit outside the core, provided they operate to common standards and can reuse core capabilities without fragmented integration. These may include wallets and checkout interfaces; QR, NFC and other acceptance products; identity and trust services; alias directories; fraud analytics; dispute case management; switching services; cross-border interlinking services; and complex programmable or agentic logic.

Separation should not mean optional consistency. Where a service affects payment certainty, customer protection, fraud, refunds, disputes or merchant reconciliation, the scheme and standards layer should define interoperable minimum requirements, service levels and data exchange. The core should expose the hooks and common messages needed for those services to operate across products and providers.

Q9. Digital identity and verifiable credentials

Digital identity and credentials could improve confidence that a payer, payee or merchant is the intended counterparty, reduce misdirected payments and impersonation fraud, and support attribute-based use cases such as delegated authority or age and eligibility checks without repeatedly sharing full identity information.

The challenges are equally material: privacy, consent, data minimisation, accessibility, false matches, liability for incorrect credentials, revocation, governance, cross-scheme interoperability and integration cost. Identity requirements should be proportionate to transaction value and risk. For low-value, low-risk purchases, an additional checkout field or verification step may cause more abandonment than it prevents in fraud; identity should therefore be risk-triggered rather than a default step. UK standards should align and interoperate with relevant European frameworks so merchants can offer comparable consumer experiences without duplicative integrations. A smartphone-only or single-provider approach could exclude users and reduce resilience. Merchants should help define use cases, acceptance standards and liability.

Q10. Other architecture-wide issues

Several issues require coordinated decisions across the full architecture rather than treatment within a single layer.

- Merchant governance: formal, continuing merchant representation in RPIB, DeliveryCo, scheme and implementation working groups.

- Commercial model: transparent, predictable and non-discriminatory pricing that supports a sustainable A2A proposition after merchant-funded implementation and change costs. Delivery plans should also address how consumers will be encouraged to use A2A once it is available.
- Liability and redress: clear, proportionate responsibilities and consistent refund, reversal, dispute and recovery processes designed for direct A2A. The design should assess requirements against A2A risks and dispute experience rather than importing other payment-method processes without considering their benefits, friction and operational cost.
- Operational consistency: common status messages, error codes, identifiers, service levels and escalation routes across banks and PSPs.
- Acceptance readiness: coordinated technical standards, certification, terminal or software compatibility and realistic merchant implementation lead times.
- Data and reporting: timely, standardised data for reconciliation, fraud management, customer support and performance measurement.
- Payment choice and accessibility: avoid mandating a single form factor or digital channel and preserve inclusive alternatives.

Q11. Approach to interoperability

MAG supports the objective that payers and payees should be able to transact across regulated forms of money seamlessly and at par, with settlement in central bank money and without requiring merchants to build separate acceptance integrations for each form of money. Any A2A or open-banking innovation should also interoperate with existing merchant systems and payment infrastructure, use common standards and deliver consistent, reliable outcomes for retailers and customers.

Interoperability should deliver consistent merchant outcomes: a definitive payment status, predictable value received, standard reconciliation data and equivalent minimum protections regardless of the payer's provider or form of money. This requires common technical and data standards, conformance testing, clear governance, transparent fees and unambiguous allocation of liability. Interoperability should expand choice rather than oblige a merchant to accept every new form of money or bear conversion, liquidity or integration risk.

Q12. Trade-offs between settlement models

From a merchant perspective, the Bank should assess wholesale settlement models against common outcomes: clear finality, near-instant payment confirmation, operational resilience and timely access to funds. MAG does not take a position on a single gross, net or hybrid model at this stage.

Detailed selection between gross, net or hybrid approaches should be supported by published impact analysis of liquidity, concentration, throughput and resilience. Whatever systemic model is chosen, it should provide unambiguous merchant confirmation and timely access to funds without imposing avoidable costs. Merchant-facing funding schedules and other bilateral terms should remain matters for merchants and their payment providers where they do not compromise safety or finality.

Q13. Governance and operational requirements for interoperability

Interoperability requires more than technical connectivity. It needs a common rulebook, accountable governance and enforceable operational standards across forms of money and product arrangements.

- Transparent eligibility, access and pricing requirements, with proportionate obligations and no discriminatory treatment.
- Common message, identifier, status, error, credential and reconciliation standards, supported by conformance certification.
- Clear rules for finality, liability, refunds, disputes, fraud response and recovery across multi-party journeys.
- End-to-end service levels, monitoring, incident communications, resilience testing and fallback arrangements.
- Coordinated change management, versioning and migration processes that include merchant and acceptance-provider readiness.
- Governance representation for merchants and other end users, with transparent decisions and conflict-management arrangements.

Q14. A2A payments at physical and online points of sale

The consultation identifies several necessary elements, including certainty of fate, speed, integration with point-of-sale infrastructure, common standards and product-level governance. However, further design work is needed before A2A at PoS can become a credible and widely accepted alternative for merchants.

A2A must deliver near-instant and unambiguous payment success or failure, with standard status and error messages across banks and PSPs. Merchants need sufficient certainty to release goods or services, as well as consistent rules for refunds, partial refunds, reversals, disputes, fraud, liability and customer redress. The design should work across in-store, e-commerce and in-app environments and support both one-time and recurring relationships.

Commercial viability is fundamental. Merchant adoption will depend on whether the all-in A2A proposition is sufficiently attractive to justify implementation and operational change. Assessment should include transaction, API, scheme, gateway and service fees; integration, hardware, certification and support; and the operational cost of refunds, cancellations, fraud, reconciliation, disputes and customer service. Protections should be proportionate to A2A risks and dispute experience rather than benchmarked mechanically against card chargeback models. Requirements imported from other payment methods should be assessed for whether their benefits justify the resulting cost and friction. Pricing and protection rules should be transparent and sufficiently clear before merchants are asked to fund implementation.

- Test high-volume, low-ticket and fast-turnaround environments, where small increases in latency or authentication friction can reduce conversion and create queues.
- Standardise authentication behaviour, decline reasons and error codes to avoid fragmented bank-by-bank experiences and unexplainable customer failures.

- Minimise changes to existing terminals and merchant software through reusable standards, while accounting for certification, deployment and support costs.
- Provide rich reconciliation, refund and exception data with stable transaction identifiers.
- Preserve merchant and consumer payment choice; adoption should be earned through better outcomes rather than mandated.

Q15. Cross-border payment design

The next-generation infrastructure should use internationally compatible messaging and data standards, interoperate with relevant SEPA messaging, data and operational standards where appropriate, preserve end-to-end identifiers and transaction status, and support bilateral or multilateral links with overseas fast-payment systems. Interlinking should prioritise corridors and use cases where it can demonstrably reduce cost, delay, uncertainty and reconciliation friction for households and businesses.

Commercial arrangements should reflect merchant and consumer priorities alongside provider sustainability. Fees, foreign-exchange rates, settlement value and timing should be transparent before initiation. Governance and disclosure should help avoid unnecessary fee layering or opaque mark-ups and support a sustainable merchant proposition. Regulated banks and non-bank payment providers should have fair, non-discriminatory access, supported by routing transparency and interoperable standards. Corridor pilots should test the full merchant journey, including failures, refunds, disputes, fraud controls, traceability and reconciliation, rather than only successful transfers.

Q16. Requirements for programmable payments

The core should be compatible with programmability without embedding complex or rapidly changing business logic in the systemic clearing layer. Baseline requirements should include enriched structured messaging; conditional hold and release patterns; deterministic handling of timeouts, failures and partial completion; unique end-to-end references; and clear status, finality and audit trails.

The wider ecosystem should define consent, transparency, revocation, liability, dispute handling, security, data access and fallback rules. Programmed instructions must be understandable and controllable by the user, with limits and notifications appropriate to the use case. Performance testing should reflect high-volume and time-critical environments so additional conditions do not create unacceptable latency or new points of failure.

Q17. Safe agentic payments

Infrastructure must identify agent-initiated payments through a mandatory, standardised flag in the payment message and carry verifiable information about the initiating agent, the authorising user and the scope of delegated authority. It should also carry a standardised intent credential evidencing the user's authorisation, permitted action, value and time limits, and revocation status. Optional identification would leave the transactions that present the greatest risk least transparent. The infrastructure should support limits by value, frequency, merchant or category; real-time notifications; revocation or emergency stop mechanisms; complete audit trails; and consistent failure, dispute and recovery processes.

The principal adoption barriers are unclear accountability and liability, inconsistent authentication and delegation standards, security and privacy concerns, difficulty proving the user's intent, and a lack of trusted certification or governance for agents. Agentic payments should not be treated as lower-risk

merely because they are automated. Users and merchants need clear attribution and predictable redress when an agent acts outside its authority, is compromised or makes an error.

Q18. Priority consumer-protection and fraud capabilities

MAG supports protection that is consistent across A2A routes while remaining proportionate to actual dispute incidence and sensitive to checkout friction. It should not be benchmarked mechanically against cards, where dispute volumes and obligations differ. The core should prioritise capabilities that improve prevention, transparency and recovery without prescribing a single commercial fraud solution or importing card-equivalent cost.

- Verified payee and merchant credentials, building on confirmation-of-payee concepts across interoperable routes.
- Rich, standardised and timely payment data, including consistent payer and payee identifiers, relevant name fields, an end-to-end reference, the initiation method, and a mandatory agentic-payment flag and intent credential where applicable. This should support merchants and PSPs in fraud, AML and financial-crime prevention, customer support and reconciliation, subject to privacy and data-minimisation requirements.
- Near-real-time sharing of relevant risk signals under clear privacy, access and governance controls.
- End-to-end traceability, timestamps and standard transaction status, failure and exception messages.
- Clear responsibility hand-offs, common dispute and recovery workflows, and rapid mechanisms for freezing or recovering funds where appropriate.
- Strong authentication capabilities that can be applied proportionately and consistently, with monitoring of false declines, abandonment and impacts on low-value transactions.
- Clear attribution, limits, revocation and recovery controls for delegated, programmable and agentic payments.

IV. Conclusion

MAG supports the Board's direction towards adaptable, resilient and competitive retail payments infrastructure. The programme should ultimately be judged by whether it produces reliable merchant adoption, meaningfully improves payment choice and delivers fast, safe and commercially sustainable payment options for merchants and their customers.

MAG would welcome continued engagement with the Bank, RPIB and DeliveryCo and would be pleased to contribute a merchant perspective from members operating across the UK and wider European market. If the Board would find further merchant evidence, testing or implementation input useful, MAG can support structured engagement with members, subject to appropriate confidentiality. MAG respectfully recommends merchant representation in relevant design, rulebook, commercial-model, testing and migration working groups so that infrastructure is designed with merchants rather than around them.



4248 Park Glen Road
Minneapolis, MN 55416
(952) 928-4648

MAG appreciates the Board's consideration of the merchant perspective and looks forward to collaborating further on behalf of the merchant voice in the region as this work develops.

Respectfully,

A handwritten signature in dark ink, appearing to read 'John Drechny', with a long horizontal flourish extending to the right.

John Drechny
Chief Executive Officer
Merchant Advisory Group