

6 October 2026
Payments and Fintech Team
HM Treasury
1 Horse Guards Road
London SW1A 2HQ
Via email: Modernisingpaymentservices@hmtreasury.gov.uk

Re: Modernising Payment Services Regulation consultation

Dear Sir or Madam:

The Merchant Advisory Group (MAG) respectfully submits these comments in response to HM Treasury's consultation on modernising the regulatory framework for payment services and electronic money. MAG welcomes the Government's aim to create a clear, predictable and proportionate framework that supports innovation while maintaining security and important protections for payment users.

Merchants experience payment regulation through the practical operation of checkout, authorisation, settlement, refunds, payouts, reconciliation and disputes. Reform will succeed only if new payment methods are reliable for customers and merchants, interoperable with existing systems, commercially sustainable to accept and supported by clear responsibilities throughout the payment chain. MAG's response therefore focuses on the questions where merchants can provide a direct operational perspective.

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 more than 200 of the world's leading merchants across industries including airlines, retail, restaurants, insurance, amusement parks, grocery and software, MAG facilitates strategic engagement across North America, Europe and Asia.

This response reflects priorities identified with MAG's European merchant advisers, including merchants operating across in-store, e-commerce, in-app and recurring payment channels. MAG does not respond to Questions 7-9, 11, 14, 19, 33 and 37-39, which primarily concern authorisation, prudential, competition-law or supervisory matters beyond the direct merchant perspective.

II. MAG's Overarching Priorities

Reliability and payment certainty. A merchant should receive a near-instant, unambiguous and reliable status before releasing goods or services. Standard identifiers, status messages, error codes and traceability should follow a payment through initiation, authorisation, execution, refund, reversal, payout and reconciliation.

Interoperability and proportionate standardisation. Open Banking, tokenised and agentic payments should interoperate with existing systems and use common data and interface standards. Relevant UK standards should remain aligned with European and international developments, including SEPA, while preserving UK operational resilience and payment sovereignty.

Commercial sustainability and choice. New payment methods will scale only where the all-in cost and implementation burden are transparent and proportionate to the service provided. Merchants should retain choice over the payment methods they accept and should not face discriminatory access terms or opaque layers of cost.

Proportionate protection. Authentication, liability and redress should reflect the actual risks and dispute incidence of each payment type. Importing card-specific requirements without evidence could add cost and friction without improving outcomes. Customer and merchant protections should nevertheless be clear and consistently applied across providers. For example, one digital-goods merchant reported no chargebacks over a 12-month period on the instant account-to-account methods it accepted in Europe. In that merchants' experience, the more important protection is a reliable refund route linked to the original payment, rather than automatic replication of a card-style chargeback process.

Merchant participation. Merchants fund implementation and manage the customer-facing consequences of payment design. They should therefore have formal representation in the Future Entity, commercial scheme governance, technical working groups and implementation planning.

III. Responses to the Consultation Questions

Questions 1-4: Legislative framework, definitions and international alignment

Question 1. Core rights and obligations should remain in legislation where they provide durable certainty about access, authorisation and consent, execution, liability, refunds, redress and non-discrimination. More detailed and technical requirements - including authentication methods, interface specifications, payment-status data, service levels, testing and version management - are better suited to FCA rules that can evolve through transparent consultation. Requirements that materially affect payment certainty, liability or access should not be changed solely through guidance.

Question 2. Existing provisions should be updated to support outcomes-based authentication, consistent payment-status and error information, end-to-end transaction identifiers, clear refund and reversal processes, and allocation of liability across increasingly complex payment chains. Where currency conversion is offered, customers and merchants should receive clear pre-transaction information on the exchange rate, mark-up, fees and expected amount. Any transition should include adequate notice, conformance testing and coordinated change windows so merchants can manage integration and operational risk.

HM Treasury should also examine whether the Strong Customer Authentication exemption framework gives merchants sufficient ability to benefit from their own fraud performance. Transaction Risk Analysis exemptions rely materially on payment-service-provider or acquirer fraud thresholds, leaving an individual low-fraud merchant with limited control over whether frictionless treatment is available. The UK should consider whether standardised merchant-level performance data could support more targeted exemptions, subject to safeguards, consistent measurement and issuer risk controls. Merchant-level approaches used in European markets, including France's Safe'R by CB programme, merit examination. The objective should be to reduce unnecessary friction and false declines while maintaining effective fraud prevention.

As the FCA would be responsible for developing much of the detailed framework, HM Treasury should ensure that merchants are involved early in the FCA's design work, particularly any review of SCA exemptions and fraud thresholds. MAG would welcome the opportunity to contribute merchant evidence and convene the regional merchant voice in those discussions.

Question 3. Definitions should be technology-neutral and broad enough to cover tokenised funds, Variable Recurring Payments (VRP), agentic or delegated initiation, merchant payouts and programmable payment functionality. Definitions should focus on the economic function and customer outcome rather than the underlying technology. They should also avoid gaps or overlaps that require merchants to build different processes for functionally equivalent payments.

Question 4. The UK should remain aligned, where appropriate, with EU payment-services reform, SEPA requirements, digital identity developments and relevant work on the digital euro. Global merchants should not be required to build materially incompatible journeys or data processes for neighbouring markets without a clear risk-based reason. Alignment should be pursued alongside domestic resilience, competition and payment-sovereignty objectives.

Questions 5-6: Tokenised deposits and stablecoins used for payments

MAG does not take a position on the precise regulatory perimeter for tokenised deposits or stablecoins. From a merchant perspective, however, any instrument presented as money-like for retail payments should provide clear value and redemption certainty, finality, settlement timing, transparent total cost, reliable refunds and disputes, and end-to-end traceability. It should interoperate with established acceptance and reconciliation processes, and acceptance should remain a merchant choice.

Where an overseas jurisdiction is recognised, equivalent outcomes should apply throughout the payment chain, including clarity on the responsible entity, consumer and merchant recourse, operational resilience and the treatment of a failure or loss of value. A recognised instrument should not create a lower-protection route for a payment that is functionally equivalent to a domestic transaction.

Question 10: Technology-neutral regulated activities

MAG supports technology-neutral regulation where equivalent activities and risks produce equivalent outcomes. A common framework can reduce fragmentation and avoid forcing merchants to maintain separate operational models for tokenised and non-tokenised payments. It should not, however, assume that the risks are identical in every case. Requirements for finality, status information, safeguarding, redemption, operational resilience and liability should remain proportionate to the instrument and payment chain, while delivering a consistent minimum outcome to the merchant and customer.

Questions 12-13: Smart contracts, programmable payments and conduct

Programmable payments could support useful merchant and customer journeys, but the regulatory framework should establish a dependable baseline. The payment instruction and any condition should be understandable; consent should be explicit and auditable; authority should be revocable where the payment has not become irrevocable; and the system should define what happens when a condition fails, is partly completed or times out. Merchants also need clear finality, notification, refund, dispute and liability rules, together with a safe fallback when automated execution does not complete as intended.

Conduct outcomes should be consistent across tokenised and conventional retail payments. This includes transparent terms, reliable status and reconciliation information, accessible support, error handling, refunds and reversals, and an auditable record. These protections should not be interpreted as a requirement for merchants to accept a particular tokenised instrument.

Question 15: Agentic payments

Agentic payments should be designed around verifiable customer intent and clear attribution. The payment message should include a mandatory, standardised indicator that an agent initiated the transaction, together with the identity or credential of the agent and principal, the scope of authority and a verifiable intent credential. An optional indicator would not provide a reliable control because the transactions that omit it may be those for which attribution matters most.

Customers should be able to set limits by value, frequency, duration, merchant or category; review and revoke authority; and use an emergency stop. Merchants should receive enough information to assess whether the

transaction is within the mandate without receiving unnecessary personal data. The liability chain should be explicit where an agent acts outside its authority, an identity or credential is compromised, or the merchant fulfils in reasonable reliance on a valid instruction. Automated replenishment and other recurring use cases should be included from the outset rather than deferred.

Mobile top-ups and in-game balances are likely early use cases, including an agent replenishing a prepaid balance when it falls below an agreed level. Because fulfilment may be instant, the agent indicator, mandate scope and verifiable intent credential must reach the merchant with the payment authorisation, rather than afterwards. Identity checks should remain proportionate to value and risk: a low-value top-up made within an existing mandate should not require full re-verification on every occasion.

Liability rules should distinguish between a compromised agent or credential, an agent exceeding its mandate, incomplete or ambiguous customer instructions, an agent incorrectly interpreting those instructions and a merchant failing to fulfil the resulting order. A merchant that correctly fulfils an authenticated instruction within a valid mandate should not bear responsibility for customer dissatisfaction caused by the agent's interpretation of the customer's instructions. Rules should specify the evidence, refund, dispute and redress process applicable to each scenario.

Question 16: Other innovation

The framework should be capable of accommodating digital identity and reusable credentials, request-to-pay, commercial VRP, payout flows and richer standardised payment data. Common components should be modular and interoperable so innovation does not create closed systems or require duplicate merchant integrations. Standards for consent, initiation attribution, payment status, error handling, refunds, reconciliation and fraud-prevention data should apply consistently across relevant use cases.

Question 17: Inclusive payments

MAG does not represent itself as a specialist organisation for vulnerable consumers. Merchants can nevertheless offer an important operational perspective on whether payment journeys work at the point of interaction. Modernisation should not make smartphone ownership the only practical route to payment, and customer journeys should support accessibility tools and viable alternatives. Authentication should be proportionate to transaction value and risk; for low-value purchases, an unnecessary field or verification step can create more abandonment than fraud prevention. Regulators should test new requirements with specialist consumer groups and monitor abandonment, false declines and inability to complete a payment across channels.

Questions 18 and 20: Emerging risks and targeted amendments

The principal merchant-facing risks include inconsistent interfaces and data, ambiguous payment status, unclear liability, insufficient fraud-prevention information, concentration or fragmentation among providers, operational outages and opaque cost layering. These risks become more significant as a single payment passes through more technical and commercial intermediaries.

Targeted amendments should support:

- outcomes-based, risk- and value-proportionate authentication;
- standard data fields, end-to-end identifiers, status messages and error codes;
- clear allocation of responsibility for fraud, errors, refunds, reversals and disputes;
- consistent conformance testing, operational resilience and change management; and
- proportionate requirements based on evidence of the risks and dispute incidence of the payment type.

Question 21: A right of access to Variable Recurring Payments

MAG supports establishing a clear right of access to VRP functionality. Broad and dependable coverage across relevant account providers is essential if merchants are to invest in commercial account-to-account payment journeys. Fragmented availability would make the payment method difficult to explain to customers and could require merchants to maintain inconsistent checkout and mandate-management processes.

The right should support practical use cases including subscriptions, utilities, travel, digital services and variable bills. Common standards should cover mandate creation, amendment and revocation; customer notification; retries and insufficient-funds handling; refunds and reversals; payment certainty; and reconciliation. These requirements should be designed with merchant participation and tested across customer channels and merchant sectors.

Travel provides a practical example of demand for flexible recurring functionality. One MAG travel adviser reports that approximately 70 percent of guests select a Reserve Now, Pay Later option where it is available. VRP could also support split and group payments, creating more convenient customer journeys while reducing reliance on card rails and operationally cumbersome workarounds.

Questions 22-23: Charging and contractual access

MAG's preference is for access currently required by statute to remain free. Proportionate charging may be appropriate for genuinely additional commercial services where they deliver demonstrable value to customers or merchants, but pricing should be cost-reflective, transparent and non-discriminatory. Assessment should consider the merchant's all-in cost, including implementation, integration, certification, transaction processing, scheme or intermediary charges, reconciliation and ongoing change, as well as the benefits delivered to customers.

Lower cost alone will not ensure customer adoption. One MAG travel adviser reported adoption below 0.5 percent during a UK Pay by Bank test and identified the absence of familiar purchase protections as a likely barrier. Providers have suggested that merchants use acceptance savings to fund customer promotions, but continuing merchant-funded incentives are not a sustainable substitute for inherent customer value. A fair-value approach should consider whether the price is reasonable relative to the service and benefits provided.

Account-to-account payments are also not automatically cheaper in every operational respect. Where a method lacks a native refund route, each refund may require the merchant to collect the customer's bank details and initiate a separate transfer. One digital-goods merchant reports that this can require 10-15 minutes of staff time per refund, compared with a few minutes where the refund can be executed through the original payment rail. Lower acceptance cost is an important offsetting factor; additional access charges could materially weaken the commercial case for adoption.

MAG is concerned by the suggestion in paragraph 4.16 that charging could apply when API-call volumes exceed a high threshold. A volume threshold could disproportionately affect high-frequency, low-value sectors such as digital goods, where any resulting per-transaction charge represents a larger proportion of the purchase value. Status enquiries, refund requests and other remedial calls should not count towards a threshold, particularly where those calls result from incomplete or delayed information supplied by an account provider. Any threshold should also account for transaction value, efficient cost to serve and interface quality.

MAG would not support a general requirement for bilateral contracts as a condition of baseline access. Bilateral negotiation can create delay, inconsistent rights and barriers for smaller participants. If contracts are permitted for genuinely additional or higher-value commercial services, they should be based on standard

multilateral terms, should not allow refusal or delay of baseline access, and should include transparent service levels, liability and dispute processes.

Questions 24-27: Access rights, definitions and legislative safeguards

Open Banking access rights should be supported by practical service obligations. MAG welcomes the recognition in paragraph 4.17 that the payment-status information provided to payment-initiation service providers may be insufficient. Encouragement alone is unlikely to produce the consistency merchants require; accurate, reliable and timely status information should be an enforceable requirement. A merchant or its provider should receive standard error information, a consistent transaction identifier and a near-instant, definitive and machine-readable outcome before releasing goods or services.

Standards should distinguish clearly between terminal statuses, such as succeeded or failed, and any genuinely non-terminal status. A pending or uncertain status should not be presented as authority to fulfil an order, should be subject to a defined resolution period and should transition automatically to a definitive outcome. This is particularly important for digital goods such as mobile top-ups and game credits, which may be delivered automatically within seconds and cannot readily be recovered.

A refund should be a standard function executed as a linked reversal referencing the original payment, rather than a new outbound payment requiring the customer's bank details. The merchant's own transaction reference should be preserved unchanged from initiation through settlement, with end-to-end traceability covering refunds, reversals, disputes, payouts and reconciliation. One merchant reports that a provider's settlement files omit the merchant reference and split individual payments across multiple rows, requiring manual matching.

Definitions should be sufficiently future-proof to cover VRP, agentic or delegated initiation and relevant payout flows without creating gaps between functionally similar services. Core rights of access, non-discrimination, liability and user protection should remain in legislation. Detailed interface, data, service-level and conformance requirements can be set by the FCA, subject to consultation and appropriate implementation periods.

The framework should also provide for published service levels, conformance testing, version management and coordinated change windows. Merchants and their providers should not bear repeated implementation costs because participants adopt inconsistent versions or interfaces.

Questions 28-29: FCA interface powers and scheme participation

MAG supports FCA powers to set and enforce interface, resilience, service-level, performance, conformance and change-management requirements. The objective should be consistent customer and merchant outcomes, not merely technical availability. Measures should include response times, uptime, definitive payment status, error quality, successful completion, refund performance and the stability of production interfaces.

Although voluntary arrangements may be given an opportunity to develop, the FCA should retain a proportionate reserve power to require participation where evidence shows that limited coverage is preventing a viable market. The power should be used transparently and after consultation, but the absence of broad account-provider coverage should not become a permanent barrier to merchant and customer adoption.

Questions 30-31: Product data and sweeping VRPs

Product and reference information should remain available where it supports customer choice and payment functionality, provided the information is relevant, current, standardised and machine-readable. Requirements should focus on data quality and practical use rather than volume of publication.

Existing sweeping VRP functionality should remain available and reliable. It should not, however, be treated as a substitute for wider commercial VRP. The two uses can share common standards for consent, mandate management, status and revocation while retaining rules appropriate to their different purposes and risks.

Question 32: Regulation and governance of the Future Entity

MAG supports appropriate FCA regulation of the Future Entity. Its governance should be transparent and accountable, with formal representation for merchants and other end users rather than engagement only through providers. Decision-making should publish objectives, evidence, performance measures and reasons for material changes. Technical and commercial working groups should include merchants of different sizes and sectors, because operational requirements and implementation costs vary materially across use cases.

Questions 34-36: Pricing powers and commercial Open Banking schemes

The FCA should have a consistent backstop power to address pricing concerns both within and outside commercial schemes. Any intervention should be evidence-based and proportionate, but the regulator should be able to examine the full chain of charges where access terms or pricing undermine competition or adoption. Transparency, comparability and non-discrimination should be baseline expectations.

Commercial Open Banking schemes should be subject to appropriate requirements for governance, access, resilience, transparent pricing, service levels and dispute resolution. Additional FCA powers should support conformance testing, standard payment-status and fraud-prevention data, version and migration management, redress and interoperability. Requirements should be coordinated to avoid unnecessary duplication across schemes and the wider retail-payments programme.

Merchant costs can scale with the number of connections as well as transaction volume. For example, one merchant's reconciliation tooling is priced according to each connected provider or payment method, meaning that every additional scheme creates a fixed cost regardless of its level of use. Multiple schemes operating with different interfaces, identifiers or data formats would multiply these costs. Common standards and interoperability should therefore be required across schemes.

Questions 40-41: FCA objectives

The FCA's objectives should be applied to Open Banking in a way that measures outcomes for customers and merchants, including reliability, choice, access, total cost, resilience and the ability to resolve errors. An innovation or data objective should not be pursued in isolation. It should operate alongside consumer protection, competition, operational resilience and proportionate treatment of firms and end users. Material standards should be developed through transparent consultation with merchants and other affected groups.

Question 42: Wider feedback and implementation

The reforms should be coordinated with the Retail Payments Infrastructure Board, DeliveryCo, the Future Entity and relevant European initiatives. Payment-service regulation, infrastructure design and commercial scheme rules will be experienced by merchants as one operating environment; inconsistent timelines or standards would create avoidable cost and risk.

Implementation should be readiness-led, include pilots across merchant sectors and channels, and publish clear dependencies and success measures. Those measures should include completion rates, latency, ambiguous status, false declines, refunds, reconciliation quality, outages and total implementation and acceptance cost, rather than technical throughput alone. Existing payment choice should remain available until replacement services are demonstrably reliable and commercially sustainable.

Pilots should explicitly include e-commerce and in-app journeys as well as physical points of sale. Online journeys differ materially: the customer is not physically present, fulfillment is often instant and automated, and refunds and disputes are handled remotely. A design demonstrated successfully in-store should not become the default for online commerce without evidence from representative online and in-app use cases.

MAG would welcome continued engagement with HM Treasury and the FCA, including opportunities to convene the merchant voice in the region as policy, rules and technical standards are developed. Early merchant participation will help ensure that reforms translate into reliable customer journeys and practical, competitive payment acceptance.

IV. Conclusion

MAG supports the Government's objective of a modern, competitive and future-ready payments framework. The opportunity is not only to enable new technologies, but to ensure that they deliver reliable, interoperable and proportionate payment services that merchants and customers can use with confidence. MAG encourages HM Treasury to preserve clear statutory rights, equip the FCA to maintain common technical and commercial standards, and build formal merchant participation into the next stages of reform.

MAG appreciates HM Treasury's consideration of the merchant perspective and would be pleased to provide further practical input as the proposals are developed.

Respectfully,



John Drechny
Chief Executive Officer
Merchant Advisory Group