

TauriPay, a Public Benefit Corporation

September 8, 2026

Retail Payments Infrastructure Board

Payments Innovation and Fintech

Bank of England

Threadneedle Street

London EC2R 8AH

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

Consultation published 25 June 2026; response deadline 11 September 2026

Response on Operational Assurance, Interoperability and Future Retail Payments Infrastructure

To the Retail Payments Infrastructure Board:

TauriPay, a Public Benefit Corporation respectfully submits this response to the Retail Payments Infrastructure Board (“RPIB”) consultation on the design of the United Kingdom’s next-generation retail payments infrastructure.

TauriPay supports the RPIB’s objective of developing core infrastructure that remains secure, resilient and trusted while enabling innovation, competition, interoperability, and new payment journeys. The present design stage provides an important opportunity to establish the operational properties that the future infrastructure should deliver before implementation choices become fixed.¹

The consultation appropriately approaches this task through three complementary perspectives: future payment journeys, design principles, and the core infrastructure’s role within the wider payments ecosystem. The RPIB also makes clear that the design principles should guide design choices rather than prescribe technical solutions, and that the RPIB itself does not set regulatory requirements.²

TauriPay’s principal observation is:

The design of next-generation payment infrastructure should begin by defining the outcomes and operational properties that the complete payment journey must preserve, including under stress, and then determine which architectures and dependencies can satisfy those requirements.

This becomes increasingly important as the payments ecosystem becomes more heterogeneous. The Payments Vision Delivery Committee (“PVDC”) expressly contemplates a diverse multi-money ecosystem with interoperability between new and existing forms of digital money, while the consultation contemplates regulated stablecoins and other regulated private-money issuers participating in the future infrastructure.³

Different forms of money may perform economically similar functions while depending upon materially different mechanisms for ordering, completion, availability, recovery, and determination of transaction state.

¹ Bank of England, RPIB consultation on the Design of the Future Retail Payments Infrastructure (25 June 2026) (RPIB Consultation), Foreword and Section 1. The consultation explains that the RPIB is translating the National Payments Vision and PVDC Strategy into the high-level design for the next-generation core infrastructure, which will be taken forward by the industry-led Delivery Company.

² RPIB Consultation, Section 1, Purpose of this consultation. The consultation approaches the design through future payment journeys, design principles and the wider payments ecosystem; the principles are intended to guide rather than prescribe specific technical solutions. The RPIB states that it does not set regulatory requirements.

³ RPIB Consultation, Table A and Sections 1-2. PVDC Outcome 2 calls for payments to operate seamlessly in a diverse multi-money ecosystem with interoperability between new and existing forms of digital money. The consultation contemplates regulated stablecoins and other future forms of money within that ecosystem.

Three principles therefore inform this response:

Technology neutrality should not imply operational equivalence.

Interoperability creates dependency. Material dependency requires proportionate operational assurance.

The relevant unit of operational assurance should be the end-to-end payment journey, including its material dependencies, rather than each component considered in isolation.

These principles do not favour a particular technology or architecture. They are intended to ensure that the properties upon which users, institutions, and the wider financial system rely remain explicit, measurable, and testable as payment architectures evolve.

For purposes of this response, a material dependency is a system, service, infrastructure component, or control function whose failure, degradation or material change could materially affect completion, certainty of fate, settlement finality, availability, reconciliation, or recovery of a supported end-to-end payment journey.

For purposes of this response, authoritative state means the record or determinable system state relied upon to establish the status and outcome of a payment where participants or infrastructure components disagree, or where payment state must be reconstructed following disruption.

Executive Summary: Key Observations and Recommendations

TauriPay supports the RPIB's technology-agnostic approach and its focus on resilience, interoperability, innovation, and end-user outcomes. Our response adds an operational-assurance perspective intended to help translate those objectives into properties that can be observed, tested, and reassessed as the future payments ecosystem evolves.

TauriPay approaches these questions from the perspective of both UK and global financial-market infrastructure. The United Kingdom's position as a global financial centre means that the design of its next-generation payments infrastructure will operate within an increasingly interconnected ecosystem of domestic and cross-border payment systems, new forms of digital money, programmable platforms, and financial-market infrastructure.

The RPIB process therefore provides an opportunity to identify material operational properties and dependencies at the design stage, before new arrangements become embedded in critical financial activity. Our comments are intended to support that objective by focusing on how payment outcomes, infrastructure dependencies, and assurance requirements can change as functions are distributed across heterogeneous systems.

Four observations frame the response:

- 1. Economic equivalence does not imply operational equivalence. Economically similar forms of money may depend upon infrastructures with materially different characteristics for capacity, ordering, completion, finality, recovery, and control.**
- 2. Instantiation creates material dependencies, and interoperability connects those dependencies. The relevant assurance perimeter should therefore follow the functions required to produce the end-to-end payment outcome.**
- 3. Fitness for purpose should be demonstrated under realistic scale and stress before critical reliance develops. Assessment should be capable of identifying not only risks that can be mitigated, but circumstances in which an infrastructure, dependency or interoperability arrangement is not presently suitable for a contemplated function or scale.**
- 4. Assurance should continue after deployment. As transaction volumes, dependencies, interoperability arrangements and underlying technologies change, material operating assumptions should be supported by operational evidence and reassessed where necessary.**

These observations are intended to preserve architectural choice while ensuring that material operating characteristics remain explicit, measurable and capable of reassessment as the ecosystem evolves.

Contents

Executive Summary	3
<i>Key observations and recommendations</i>	
I. Payment Journeys	5
<i>Define the outcomes the complete journey must produce</i>	
II. Observable Operational Requirements	7
<i>Translate resilience and scalability into measurable properties</i>	
III. End-to-End Operational Assurance.....	10
<i>Follow the complete payment journey and its material dependencies</i>	
IV. Instantiation, Interoperability and Material Dependencies	11
<i>Identify where operational characteristics and dependencies reside</i>	
V. Failure, Stress, Change and Continuing Fitness for Purpose	15
<i>Measure before criticality; test at scale and reassess through change</i>	
VI. Cross-Border Interlinking.....	17
<i>Preserve end-to-end state visibility across connected infrastructures</i>	
VII. Identity, Programmability and Agentic Payments	18
<i>Keep authority, state and accountability explicit</i>	
VIII. Consumer Protection and Fraud Capabilities.....	20
<i>Provide common evidence and control primitives in the core</i>	
IX. Recommended Additions to the High-Level Design.....	21
<i>Translate the analysis into design and requirements considerations</i>	
Conclusion.....	22
<i>Preserve architectural choice while making required outcomes demonstrable</i>	

I. Payment Journeys Should Specify Outcomes, Not Merely Functions

Relevant consultation questions: 1, 2 and 14

TauriPay supports the RPIB's decision to ground the high-level design in concrete payment journeys and end-user outcomes. The consultation identifies existing and emerging journeys including immediate payments, batch and recurring payments, cross-border payments, A2A at point of sale, delegated payments, programmability and interoperability across forms of money.⁴

We recommend that these journeys ultimately specify not only the functionality the infrastructure must support, but also the operational states and outcomes that must be preserved throughout the payment lifecycle.

Depending upon the architecture, relevant states may include:

instruction → acceptance → ordering → execution → confirmation → settlement/finality → availability of funds

These states need not be separate in every architecture. Some may coincide.

The important requirement is that the infrastructure establish clearly, where relevant:

- what operational state a payment has reached;
- whether it has succeeded, failed, or remains unresolved;
- when the payer and payee have certainty of fate;
- when it is considered complete;
- when settlement finality occurs;
- when the recipient may rely upon the funds;
- which record or state is authoritative;
- what occurs if participating components report inconsistent states; and
- how the transaction and its outcome can subsequently be reconstructed.

The Bank's distinction between certainty of fate and settlement finality is particularly useful. The consultation defines certainty of fate as reliable confirmation to payer and payee that a payment succeeded or failed, and separately defines settlement finality as the point at which a payment or transfer becomes final, irrevocable and unconditional, such that it cannot be reversed and the payment obligation is discharged.⁵

A payment journey may therefore require rapid certainty of fate for an end user while the execution infrastructure separately establishes when the underlying payment reaches settlement finality.

Where certainty of fate, operational completion and settlement finality do not coincide, the high-level design should make those distinctions explicit.

This is particularly relevant to A2A at point of sale, where the consultation identifies certainty of fate, speed and reliability as necessary outcomes and contemplates near-instant confirmation sufficient for a merchant to release goods or services.⁶

⁴ RPIB Consultation, Section 2, Figure 4 and Questions 1-2. The proposed journeys include immediate, batch, recurring and cross-border payments and emerging A2A at PoS, delegated payments, programmability, deferred payments and interoperability across forms of money.

⁵ RPIB Consultation, Section 4 and Annex 1. 'Certainty of fate' is defined as reliable confirmation to payer and payee whether a payment succeeded or failed. 'Settlement finality' is defined as the point at which a payment or transfer becomes final, irrevocable and unconditional, such that it cannot be reversed and the payment obligation is discharged.

⁶ RPIB Consultation, Section 4, Account-to-account at point of sale. The consultation states that A2A at PoS would need certainty of fate, speed and reliability and may require near-instant confirmation sufficient for merchants to release goods or services.

I-A. Migration

The same outcome-based discipline should apply to migration.

The consultation recognises the challenges involved in moving financial institutions to next-generation infrastructure and contemplates staged transition, potentially including a defined and time-limited period of dual running where necessary.⁷

Migration decisions should therefore be supported by:

- measurable readiness criteria;
- evidence of representative-volume and stress testing;
- evidence of recovery and rollback procedures;
- evidence of reconciliation between existing and new infrastructure;
- coordinated operational transition; and
- clear exit criteria for ending any period of parallel operation.

Migration should ultimately be governed by demonstrated operating readiness, not only calendar milestones.

⁷ RPIB Consultation, Section 2, Product roadmap and transition plans. The consultation discusses orderly migration and a possible staged transition, including a defined and time-limited period of dual running where needed.

II. Design Principles Should Translate Into Observable Operational Requirements

Relevant consultation questions: 3 and 4

TauriPay supports the RPIB's proposed principles, including innovation and competition, open access, common utilities and standards, security and resilience, performance and scalability, and protection from fraud and wider financial crime.⁸

The consultation states that the future core should support high-speed processing and high throughput and should be scalable so that it can handle sustained increases in transaction volumes without degrading performance.⁹

TauriPay strongly supports this formulation. We recommend carrying it one step further by defining the production measurements through which those properties can be demonstrated.

II-A. Capacity and Scalability

Capacity should reflect the ability of the complete payment journey to process required workloads within defined service levels under representative operating conditions.

Relevant measurements may include:

- sustained end-to-end capacity;
- peak capacity and duration;
- latency under increasing load;
- queuing behaviour;
- successful completion rates;
- unsuccessful or unresolved transaction rates;
- reattempt rates;
- effective workload produced by reattempts;
- degradation under stress; and
- recovery following degradation.

This distinction matters because underlying economic payment demand and infrastructure workload can diverge during periods of stress.

Under stressed or degraded conditions, unsuccessful or delayed instructions may generate automated or manual reattempts. Those reattempts can increase offered load beyond the underlying level of economic payment demand.

Capacity and stress testing should therefore measure reattempt-generated workload, rather than treating each original payment instruction as the complete measure of demand.

II-B. Functional Demonstration and Isolated Performance Measurements Should Be Distinguished From Production Readiness

Experimentation, laboratory testing, and component-level performance measurement play an important role in establishing technical feasibility and characterising individual system components. Their evidentiary value, however, should remain aligned with what was actually tested.

⁸ RPIB Consultation, Section 3. Proposed design principles include a platform for innovation and competition, open access, common utilities and standards, security and resilience, performance and scalability, and protection from fraud and wider financial crime.

⁹ RPIB Consultation, Section 3, Performance and scalability. The consultation states that the core should support high-speed processing and high throughput and should handle sustained increases in transaction volumes without degrading performance.

A successful functional demonstration may establish that a business workflow can execute as intended. Similarly, an isolated performance measurement may establish the throughput, latency, or computational performance of a particular system component under specified conditions. Neither, without further end-to-end lifecycle validation, necessarily establishes the sustained capacity or operational performance of the complete payment journey under representative production conditions.

End-to-end performance may be affected by interactions not captured in isolated measurements, including concurrency, participant distribution, network conditions, dependencies, sequencing, unsuccessful transactions and reattempts, state propagation, reconciliation, recovery, and other operational controls.

Performance evidence used to support infrastructure design decisions should therefore distinguish what was measured from what is being inferred. Where a claim concerns the capacity, resilience, or fitness for purpose of the complete payment journey, the supporting evidence should progressively reflect the complete lifecycle and the conditions under which the infrastructure is expected to operate.

Where material performance evidence is used to support a design or fitness-for-purpose conclusion, it should preserve sufficient measurement provenance to identify what was measured, where and under what conditions it was observed, and the conclusion being inferred from the result. A fitness-for-purpose conclusion should not exceed what the available evidence demonstrates.

Functional feasibility, component performance, end-to-end performance, and production readiness are related but distinct forms of evidence. Demonstrating one should not, without appropriate validation, be treated as demonstrating the others.

II-C. Transaction State and Finality

Design requirements should also make explicit, where relevant:

- acknowledgement;
- confirmation;
- certainty of fate;
- clearing;
- settlement finality;
- unresolved states; and
- the ability to reconstruct authoritative transaction state following disruption or disagreement.

The objective is not to require every architecture to implement identical processing stages. It is to ensure that the states material to the payment outcome are observable and understood.

II-D. Recovery

The consultation appropriately states that the future infrastructure should clear payments reliably during disruptive events, detect security and resilience issues, limit their impact, and recover quickly.¹⁰

Resilience should therefore include observable recovery properties rather than uptime alone.

Relevant measures may include:

- recovery time;
- reconciliation following disruption;
- restoration or reconstruction of authoritative state;
- treatment of incomplete or duplicate instructions;
- degraded-mode operation; and
- return to normal processing.

¹⁰ RPIB Consultation, Section 3, Security and resilience. The future core is expected to clear payment volumes reliably during disruptive events, including high-severity cyberattacks, prolonged third-party outages and technical failures, while detecting issues, limiting impact and recovering quickly.

This leads to an important distinction:

Technology neutrality should not imply operational equivalence.

Different technologies may perform the same economic function while exhibiting materially different characteristics concerning completion, ordering, capacity, technical finality, failure, recovery, governance, and operational control.

The purpose is not to impose identical performance characteristics across architectures. It is to ensure that differences material to the payment outcome are visible and understood.

III. The End-to-End Payment Journey Should Be the Unit of Operational Assurance

Relevant consultation questions: 5–8 and 10

TauriPay broadly supports the RPIB’s technology-agnostic conceptual architecture.

The consultation recognises that the core clearing and messaging infrastructure is one layer within a wider payments ecosystem and that decisions concerning the core both shape and are shaped by the surrounding ecosystem. It also identifies cross-cutting design issues requiring coordination across multiple layers.¹¹

Operational assurance should therefore traverse relevant infrastructure boundaries rather than stop at them.

A payment can depend upon several components, each operating within its individual specification, while the complete payment journey nevertheless fails to deliver its required outcome.

The relevant assurance question is therefore not merely:

Did each component operate correctly?

It is also:

Did the complete payment journey produce the required outcome?

For material interfaces, the design should make explicit:

- the state entering the interface;
- the expected state following successful hand-off;
- responsibility for the hand-off;
- relevant timestamps;
- failure and timeout behaviour;
- reconciliation requirements;
- recovery responsibility; and
- the authoritative record or state where components disagree.

For each material state, the design should identify who or what establishes it, how it is observed, and what evidence can safely be relied upon.

The consultation recognises the importance of standardised transaction data, traceability, initiation-method attribution, and clear coordination as payment journeys become more interoperable and automated.¹²

TauriPay supports those concepts and recommends extending the same discipline to operational assurance.

Where a function outside the formal core becomes material to completion of a supported payment journey, the high-level design should identify which core outcomes remain invariant and which additional dependencies the external function introduces.

For example, an A2A point-of-sale journey may depend on an external function to communicate certainty of fate to the merchant. If the core processes the payment correctly but that function is unavailable, delayed, or inconsistent with the core, the merchant may still be unable to determine whether to release goods or services. That function is therefore material to the end-to-end outcome.

System-level assurance cannot be inferred solely from component-level assurance.

The operational assurance perimeter should follow the material functions required to produce the payment outcome, even where those functions cross the formal boundary of the core infrastructure.

¹¹ RPIB Consultation, Sections 1 and 4. The consultation describes the core as one layer within a wider payments ecosystem, states that core-design decisions will shape and be shaped by that ecosystem, and identifies cross-cutting design issues requiring coordination across multiple layers.

¹² RPIB Consultation, Sections 3–4. The consultation discusses common transaction data, fraud-management capabilities, identity management and delegated authorities, and the need for coordination across multi-party and increasingly automated payment journeys.

IV. Instantiation, Interoperability, and Material Dependencies

Relevant consultation questions: 10–13

Interoperability in a multi-money ecosystem is a core policy objective of the future infrastructure. The consultation contemplates different forms of regulated private money, including regulated stablecoins, accessing the next-generation infrastructure directly or indirectly, subject to appropriate assessment, governance, and contractual arrangements. It further recognises that interoperability raises design, governance and operational issues requiring coordination across the ecosystem.¹³

TauriPay supports this approach. Our additional observation concerns the operational dependencies introduced by the infrastructures through which different forms of money are instantiated and used.

From Instantiation to Continuing Operational Assurance

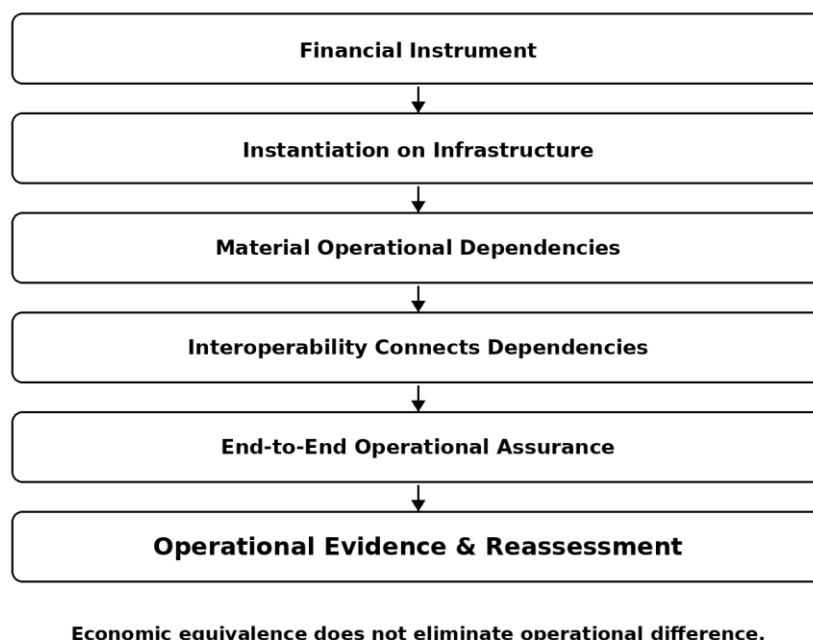


Figure 1. Instantiation, interoperability and the continuing operational-assurance perimeter.

IV-A. Instantiation Creates Operational Dependency

Where the transfer, settlement, availability, redemption, or authoritative state of a financial instrument depends materially upon a particular infrastructure, the payment journey involving that instrument necessarily depends upon relevant operational characteristics of that infrastructure.

Economically similar instruments may therefore introduce materially different operational dependencies into an interoperable payment environment.

Those differences may concern:

- ordering;
- transaction completion;
- capacity;
- availability;
- failure behaviour;

¹³ RPIB Consultation, Section 4, Interoperability between different forms of money. The consultation contemplates regulated stablecoins accessing the future infrastructure directly or indirectly, subject to assessment, risk and regulatory profile, governance and contractual arrangements, and identifies further design, governance and operational issues.

- recovery;
- governance;
- concentration;
- technical finality; or
- dependencies upon additional infrastructure.

This does not mean that an instrument inherits every technical characteristic of the infrastructure on which it is instantiated. Nor does TauriPay suggest that the legal or economic character of an instrument is altered merely because a particular technology is used. The Bank's glossary likewise notes that a tokenised bank deposit remains a claim on the issuing bank and retains the legal characteristics of a bank deposit.¹⁴

The point is narrower:

Economic equivalence does not eliminate operational difference. Where use of an instrument depends upon particular infrastructure, the operational properties of that infrastructure that are material to the payment outcome become relevant to the end-to-end payment journey.

IV-B. Interoperability Connects Dependencies

The Bank's proposed model contemplates users paying and being paid across different forms of money, with the core infrastructure enabling interoperability and settlement in central bank money.¹⁵

Interoperability should therefore be understood as more than technical connectivity.

Connecting different forms of money or infrastructure also connects the operational dependencies required for the resulting payment journey to complete.

Instantiation creates operational dependency. Interoperability connects those dependencies. Material dependencies require proportionate operational assurance.

This does not imply a centralised certification or approval model for every external technology. The level of assurance should be proportionate to the dependency's role and the consequences of its degradation.

IV-C. Settlement Models Should Be Compared on End-to-End Outcomes

The consultation notes that different payment journeys place different demands upon settlement and liquidity arrangements and asks respondents to consider trade-offs among speed, payment certainty, liquidity management, operational complexity, and scalability.¹⁶

TauriPay does not recommend prescribing a particular settlement model at this stage.

Different models may legitimately optimise different combinations of speed, liquidity, capacity, and operational complexity.

The relevant comparison should consider:

- time to settlement finality;
- liquidity requirements;
- sustainable capacity;
- queuing and backlog behaviour;
- participant-failure implications;

¹⁴ RPIB Consultation, Annex 1. A tokenised bank deposit is described as a deposit at a UK bank represented in tokenised form on a distributed or similar ledger while remaining a claim on the issuing bank and retaining the legal characteristics of a bank deposit.

¹⁵ RPIB Consultation, Section 4 and Table B. The future ecosystem is intended to support interoperability across different forms of money, with clearing and messaging capabilities enabling different forms of money to clear and settle reliably and final settlement between financial institutions taking place in central bank money.

¹⁶ RPIB Consultation, Section 4, Settlement frequency and liquidity implications, and Question 12. The consultation asks about trade-offs among settlement approaches, including speed, payment certainty, liquidity management, operational complexity and scalability.

- behaviour under degraded conditions;
- recovery characteristics;
- operational complexity;
- dependencies between clearing and settlement; and
- whether user-facing confirmation precedes final discharge.

A faster confirmation model is not necessarily a faster final-settlement model, and a higher-throughput model is not necessarily a more resilient end-to-end model.

IV-D. Layered Finality

Where an architecture contains multiple execution, confirmation or settlement layers, the payment journey should identify:

- the state upon which it relies;
- any mechanisms capable of subsequently changing that state;
- the underlying settlement dependency, where applicable;
- residual reversal, dispute, challenge or rollback mechanisms, where applicable; and
- how those technical states relate to settlement finality under the applicable payment arrangement.

The objective is not to prescribe how layered infrastructure must operate.

The payment system should know which state it is relying upon and what remains capable of changing that state.

Technical confirmation or consensus finality should not be assumed, without further analysis, to be identical to settlement finality under the applicable payment arrangement.

The design should also distinguish finality from reversibility. A payment may reach a technically or legally defined final state while remaining subject to a separate refund, dispute, compensation or other remedial process. Conversely, a technical state represented as complete may remain capable of alteration through rollback, challenge, reorganisation, administrative intervention, or another mechanism. The relevant design question is therefore not only what state a payment has reached, but what, if anything, remains capable of changing that state and under whose authority. A subsequent compensating transaction should likewise be distinguished from reversal of the original transaction state.

IV-E. Operational Accountability

Material-dependency assurance should identify how critical operational functions are governed in practice.

Relevant questions include:

- Who or what performs material operational functions?
- How is transaction ordering determined?
- How can material software, protocol or configuration changes occur?
- How are emergency actions initiated or coordinated?
- How are incidents communicated?
- How is recovery coordinated?
- How is authoritative state determined following disruption?
- What recovery procedures exist?
- How are those procedures tested and evidenced?

In conventional infrastructure, these functions may reside with an identifiable operator.

In distributed infrastructure, responsibility may be divided among multiple organisations, developers, validators, sequencers, governance mechanisms, or infrastructure providers.

Distributed responsibility should not itself be treated as a deficiency. Where responsibility is distributed, however, operational assurance should establish how incident coordination, remediation, authoritative-state determination and recovery are governed in practice.

IV-F. Effective Concentration and Common-Mode Dependency

Nominal participant or provider counts may not fully describe operational concentration.

Depending upon the architecture, relevant analysis may include:

- validator or stake concentration;
- sequencing concentration;
- software-client concentration;
- infrastructure or cloud concentration;
- governance concentration;
- critical development dependencies; and
- other control points capable of materially affecting payment outcomes.

No single decentralisation metric should substitute for analysis of effective control across material functions.

Likewise, nominally distinct services may depend upon the same ledger, cloud provider, software implementation, sequencing infrastructure, bridge, network provider, identity service, or critical software library.

Operational diversity should therefore be evaluated by the underlying dependencies rather than solely by product, participant, or provider count.

V. Failure, Stress, Change, and Continuing Fitness for Purpose

Relevant consultation questions: 3, 4, 10, 12, 13 and 16

The consultation expressly requires resilience during disruptive events, including serious cyber incidents, prolonged third-party outages, and technical failures.¹⁷

That resilience discipline should extend across the complete payment journey.

Design and assurance should consider scenarios involving:

- capacity saturation;
- unavailable participants;
- network disruption;
- delayed instructions;
- duplicate instructions;
- unresolved transaction state;
- material dependency degradation;
- partial infrastructure failure;
- correlated dependency failure;
- programmable-condition failure; and
- unsuccessful transitions between forms of money.

Expected failure behaviour, including how unresolved or indeterminate states are represented and recovered, should be considered explicitly during design rather than determined for the first time during an incident.

Material transaction state, dependency condition, and recovery status should be capable of being established within the timeframe in which participants must decide whether to retry, pause, reconcile, release funds, or resume service.

Where the correct outcome cannot safely be determined, temporarily preserving a known state may be preferable to producing an incorrect or irreconcilable result.

As stablecoins and other forms of digital money become more significant within retail payment and related settlement journeys, the operational characteristics of the infrastructure supporting those activities can become increasingly consequential. Those characteristics should be understood and measured before the underlying infrastructure becomes critical to those payment journeys, rather than discovered for the first time during a period of stress.

Where an infrastructure is contemplated as an alternative to, or material dependency of, existing payment infrastructure, its sustainable capacity, degradation thresholds, failure behaviour and recovery characteristics should be established under realistic operating conditions before critical reliance develops.

V-A. Continuing Fitness for Purpose

Assessment and experimentation should be capable of identifying not only risks requiring mitigation, but also circumstances in which an infrastructure, dependency, or interoperability arrangement is not presently fit for a contemplated function or scale. A technology-neutral framework should permit that conclusion where the evidence supports it.

Fitness for purpose is also dynamic. Capacity, completion behaviour, settlement characteristics, recovery arrangements, and dependency performance may produce materially different conclusions under scaled or stressed conditions than under controlled experimentation or initial deployment. Iterative development therefore requires iterative assurance.

¹⁷ RPIB Consultation, Section 3, Security and resilience.

V-B. End-to-End Stress Testing

Component-level testing should be supplemented by end-to-end scenario testing.

Successful laboratory or pilot results should not substitute for evidence obtained under representative scale, dependency, and failure conditions.

An illustrative scenario could assume:

1. transaction demand rises;
2. one or more material dependencies become congested or degraded;
3. latency increases;
4. unsuccessful or unresolved transactions increase;
5. users, applications and intermediaries reattempt delayed or unsuccessful instructions;
6. effective workload grows faster than underlying economic payment demand; and
7. individually functioning components collectively cease to produce the required end-to-end outcome.

The purpose is not to predict a particular crisis. It is to determine whether the combined architecture remains understandable, controllable, and recoverable when interacting operational characteristics move outside normal conditions.

System-level failure need not originate from a failed component. It can emerge from interactions among components that remain individually operational but no longer collectively produce the required payment outcome.

V-C. Material Change and Reassessment

Operational characteristics should not be assumed to remain static following deployment.

Material changes could include changes to:

- protocols;
- software;
- sequencing or consensus mechanisms;
- critical dependencies;
- governance;
- capacity;
- configuration;
- interconnection arrangements; or
- recovery mechanisms.

Where such a change could affect an operational property upon which a payment journey relies, it should trigger reassessment and, where appropriate, retesting.

Operational assurance should therefore operate as a lifecycle:

requirement → assurance → testing → deployment → operational evidence → material change → reassessment

This creates a continuing relationship between what the infrastructure was designed and tested to do, and what it can be demonstrated to do after deployment.

VI. Cross-Border Interlinking Should Preserve End-to-End State Visibility

Relevant consultation questions: 15

TauriPay supports the objective of reducing friction, delay, and cost in cross-border payments. For a global financial centre, cross-border interlinking also makes it important that interoperability preserve visibility into the state and dependencies of the complete payment journey.

The consultation identifies interlinking with domestic payment systems in other jurisdictions as one potential mechanism for improving cross-border outcomes and asks what design considerations could help address existing challenges.¹⁸

Cross-border interlinking extends the payment journey across additional infrastructures, participants, operating models, and potentially different settlement arrangements.

The high-level design should therefore support sufficient information to:

- identify where a payment resides in its end-to-end journey;
- distinguish completion of a domestic processing stage from completion of the wider cross-border journey;
- identify material dependencies at interlinking points;
- preserve relevant status information and timestamps across interfaces;
- accommodate differences in operating hours and settlement arrangements; and
- support reconciliation and recovery where participating infrastructures report different states.

The objective is not to require foreign systems to adopt identical architectures. It is to prevent interconnection from reducing visibility into the state of the complete payment journey.

Interlinking systems should not cause the operational state of the end-to-end payment to become less observable.

¹⁸ RPIB Consultation, Sections 2 and 4, Cross-border payments, and Question 15. The consultation identifies interlinking with payment systems in other jurisdictions as a potential mechanism for improving cross-border payments and asks which design considerations and solutions should be targeted.

VII. Digital Identity, Programmability, and Agentic Payments Require Explicit Authority, State, and Accountability

Relevant consultation questions: 9, 16 and 17

The consultation expressly considers digital identity and verifiable credentials, programmable payments, delegated authority, and agentic payments. It also identifies identity management, including delegated authorities, as a potential ecosystem service.¹⁹

These developments make it increasingly important to preserve distinctions among:

principal → identity → authority → initiation mechanism → instruction → execution → settlement

VII-A. Digital Identity

TauriPay supports further exploration of portable and verifiable credentials and appropriate trust-service models.

Where credentials support payment journeys, participants should be able to determine, where relevant:

- what identity or authority attribute is being asserted;
- the basis upon which the assertion can appropriately be relied upon;
- whether the assertion remains valid; and
- what evidence supports that determination.

The objective should be interoperable and auditable identity or authority evidence without unnecessary replication of underlying sensitive information.

The infrastructure itself need not determine every legal consequence associated with an identity assertion. It should provide sufficient information and evidence for applicable scheme, provider, and regulatory frameworks to make those determinations.

VII-B. Agentic and Delegated Payments

The consultation recognises that autonomous agents may initiate payments within parameters established by users and asks what capabilities or functions are needed to support agentic payments safely.²⁰

Agentic initiation changes the mechanism through which authority is exercised; it should not obscure the identity of the principal, the scope of delegated authority, the initiation method, or the resulting payment state.

The infrastructure should therefore preserve the distinction between:

- the underlying principal;
- the authority delegated;
- the mechanism initiating the payment;
- the resulting instruction; and
- the payment outcome.

An automated or agentic system does not become the economic principal merely because it generated or transmitted an instruction.

Nor does identifying the principal itself establish that every mechanism presenting an instruction is authorised to act for that principal.

¹⁹ RPIB Consultation, Section 4. The services layer includes identity management and delegated authorities, programmability and cross-border interlinking; the consultation separately discusses digital identity and credentials, programmable payments and agentic payments.

²⁰ RPIB Consultation, Section 4, Agentic payments and advanced delegation, and Question 17. The consultation defines agentic payments as payment initiation where an autonomous software agent acts on behalf of a user within parameters set by that user and asks what capabilities are required to support them safely.

Infrastructure should therefore support evidence and attribution sufficient for applicable scheme, provider, and control frameworks to make those determinations.

VII-C. Programmability

The consultation focuses on enabling programmability while maintaining resilience and user trust. It notes that conditional and event-driven payments can add processing steps, dependencies and latency and identifies failure and timeout handling, settlement finality, and legal certainty as relevant considerations.²¹

TauriPay agrees.

Programmability should not make failure semantics less explicit.

Where programmable logic becomes material to a payment journey, the architecture should establish:

- what condition is being evaluated;
- the source upon which the condition relies;
- how long the condition may remain unresolved;
- what happens upon timeout;
- what happens if a dependency becomes unavailable;
- what state the payment occupies while the condition remains unresolved; and
- what event establishes final payment completion.

External programmability should not make the underlying payment state ambiguous.

²¹ RPIB Consultation, Section 4, Programmable payments, and Question 16. The consultation notes that conditional and event-driven payments can add processing steps, dependencies and latency and identifies clear failure and timeout handling, settlement finality and legal certainty as relevant considerations.

VIII. Consumer Protection and Fraud Capabilities in the Core

Relevant consultation questions: 18

The consultation distinguishes infrastructure capabilities from the regulatory, scheme and product-level arrangements that determine how consumer protection, liability and reimbursement operate in practice and asks which consumer-protection and fraud-related capabilities should be prioritised for inclusion in the core.²²

TauriPay believes the core should prioritise the common evidence and control primitives required for participants and product-level arrangements to apply appropriate protections consistently.

These should include, as appropriate:

- persistent transaction identifiers;
- standardised transaction and status information;
- failure and reason codes;
- reliable timestamps;
- participant attribution;
- initiation-method attribution;
- end-to-end traceability;
- sufficient data fields to support fraud controls; and
- mechanisms supporting appropriate exceptions and recovery.

More complex fraud analytics, reimbursement decisions, dispute adjudication, and product-specific allocation of liability need not necessarily reside in the core.

The consultation itself contemplates fraud analytics and other services being provided either within or outside the core infrastructure.²³

The core should provide reliable evidence and common control primitives; product- and policy-specific determinations can remain with the appropriate scheme, provider, or service layer.

This preserves a focused core while ensuring that infrastructure does not become an impediment to effective protection as payment journeys become faster, more interoperable and more automated.

²² RPIB Consultation, Section 4, Consumer protection, fraud and wider financial crime, and Question 18. The consultation asks which consumer-protection and fraud-related capabilities should be prioritised for inclusion in the core and distinguishes infrastructure capabilities from wider product, scheme and regulatory arrangements.

²³ RPIB Consultation, Sections 3-4. The consultation contemplates common utilities such as fraud data analytics, some of which could be embedded within the core while others may be delivered outside it.

IX. Recommended Additions to the High-Level Design

Based on the analysis above, TauriPay recommends that the RPIB incorporate the following considerations into the high-level design and requirements process.

1. Define end-to-end payment outcomes.

Distinguish certainty of fate, operational completion, settlement finality, and availability of funds where those states differ.

2. Translate resilience and scalability into observable operational requirements.

Include sustained capacity, successful completion, unsuccessful or unresolved transactions, reattempts, latency, degradation, and recovery.

3. Treat the end-to-end payment journey as the unit of operational assurance.

Evaluate material interfaces and dependencies, including material functions outside the formal boundary of the core.

4. Apply proportionate operational assurance to material dependencies.

Assess the operational properties upon which the payment journey relies according to their materiality rather than technology labels.

5. Make layered finality, effective concentration, and common-mode dependencies explicit where relevant.

Where multiple execution or settlement layers or shared dependencies exist, identify the states, control points, and dependencies upon which the payment outcome relies.

6. Preserve end-to-end state visibility across interoperability and cross-border interlinking.

Connecting infrastructures should not make the operational state of the complete payment journey less observable.

7. Establish continuing fitness for purpose before and after critical reliance develops.

Assessment should establish sustainable capacity, degradation thresholds, failure behaviour, and recovery under realistic conditions, and should permit a conclusion that an arrangement is not presently suitable for a contemplated function or scale.

8. Require realistic end-to-end stress testing.

Include capacity pressure, degraded dependencies, unsuccessful transactions, and reattempt-generated workload rather than testing components only in isolation.

9. Reassess material dependencies following material changes.

Changes capable of affecting relied-upon operational properties should trigger appropriate reassessment and, where warranted, retesting.

10. Design for continuing operational evidence.

Important operational properties demonstrated before deployment should remain observable and capable of being evidenced after deployment and through material change.

Together, these principles establish a continuous assurance lifecycle:

requirement → assurance → testing → deployment → operational evidence → material change → reassessment

The purpose is not to prescribe how the future infrastructure must be built.

It is to ensure that what the infrastructure must reliably accomplish remains explicit regardless of how it is built.

Conclusion

The RPIB has an opportunity to make explicit, before implementation choices become fixed, the operational properties that future payment journeys must preserve regardless of architecture.

Mature payment systems have developed disciplines around capacity, state, resilience, recovery, change management and accountability over decades.

The challenge is not to replace those disciplines as new technologies are adopted. It is to determine how those disciplines should be applied when the end-to-end payment journey spans infrastructures that may implement those properties differently.

That challenge becomes particularly important in a multi-money environment.

Economic equivalence does not eliminate operational difference.

Where the use of an instrument depends upon particular infrastructure, the operational properties of that infrastructure that are material to the payment outcome become relevant to the end-to-end payment journey.

Technology neutrality should permit architectural choice without assuming operational equivalence.

Interoperability should enable innovation without obscuring material dependencies.

Operational assurance should follow the complete payment journey wherever the functions required to produce the payment outcome actually reside.

The objective is not to prescribe the architecture of the United Kingdom's future retail payments infrastructure.

It is to ensure that what the infrastructure and the payment journeys depending upon it must reliably accomplish remains explicit, measurable, and demonstrable regardless of how they are built.

TauriPay appreciates the opportunity to contribute to the RPIB's work and would be pleased to discuss these observations in greater detail.

TauriPay, a Public Benefit Corporation, consents to publication of its name as a respondent to this consultation.

Respectfully submitted,

Mark Sulavka

TauriPay, a Public Benefit Corporation