

Submission in response to the Reserve Bank of Australia's Payment System Regulation Issues Paper

Submitted by:

Paypa Plane Australia

Suite 4, Level 26, 145 Ann Street, Brisbane QLD 4000

Primary contact:

Simone Joyce

Chief Executive Officer

Email: sjoyce@paypaplane.com

Phone: +61 4395 84600

Submission Summary

Australia's payments ecosystem is becoming increasingly digital, automated and interconnected, creating new challenges and opportunities that extend beyond the payment rail itself.

This submission supports a technology-neutral, principles-based regulatory framework that promotes competition, interoperability, innovation and financial safety, while recognising the growing importance of trust, authority, consent and governance across payment systems.

It advocates for regulatory settings that enable industry-led innovation, support emerging payment models and ensure Australia's payments framework remains fit for purpose in a future shaped by digital identity, AI-enabled commerce and programmable transactions.

Executive Summary

The Australian payments ecosystem is entering a period of significant structural change. AI-enabled commerce, account-to-account payments, digital identity, tokenised forms of value, programmable money and increasingly influential global technology platforms are reshaping how payments are initiated, authorised, governed and managed.

This submission supports the objectives of the Review of Payments System Regulation and the amended PSRA by focusing on an emerging challenge that cuts across many of the issues identified in the Issues Paper. Increasingly, competition, efficiency and financial safety outcomes are being influenced not only by payment rails and settlement infrastructure, but by the trust, authority, consent and governance frameworks that sit above them.

Many of the future challenges facing Australia's payments ecosystem are no longer primarily challenges of moving value. They are challenges of establishing, evidencing and governing authority, consent, trust and liability across increasingly digital, automated and interconnected payment environments.

The submission argues that:

- effective competition increasingly depends on the portability and interoperability of payment relationships, not simply payment transactions
- future cyber resilience requires protection of payment authorities and permissions as well as payment credentials
- recurring, delegated and payer-not-present payment models create common challenges that extend across individual payment systems
- Australia should explore technology-neutral trust, authority and governance capabilities that operate across payment systems while preserving existing payment rules, liability frameworks and settlement infrastructure
- the amended PSRA provides an opportunity for the RBA to support industry-led experimentation and coordination on issues that increasingly arise above, across and beyond traditional payment rails.

The submission does not advocate replacing existing payment system rules, liability arrangements or infrastructure. Rather, it proposes a framework for improving interoperability, trust and future-readiness while preserving competition, efficiency and financial safety.

Table of Contents

Introduction	<u>4</u>
Responses to Consultation Questions	
Q6: Are there competition, efficiency and/or financial safety issues relating to the use of AI agents for payments in e-commerce? If so, are there any regulatory actions that the RBA should consider?	<u>6</u>
Q11: What are the challenges faced by participants and end-users in the A2A payments system? Do these limit efficiency, competition or financial safety in relation to A2A transactions?	<u>9</u>
Q12: Is there a case for the RBA to take any regulatory action in relation to A2A payments to support efficiency, competition or financial safety, or control risk to the financial system? If so, what regulatory actions should be considered?	<u>14</u>
Q14: What regulatory action, if any, should the RBA take to promote more standardisation and interoperability across cards and A2A payments?	<u>16</u>
Q16: What key barriers or challenges are participants facing in uplifting cryptography and broader cyber security practices?	<u>21</u>
Q17: What role could the RBA play in supporting and coordinating industry-wide cryptographic uplifts in the payments system?	<u>23</u>
19. Are there any other issues relating to payments that the RBA should consider prioritising to promote competition, efficiency and financial safety in the payments system?	
Additional Issue 1 – First-party fraud, dispute efficiency and authority verification	<u>26</u>
Additional Issue 2 – Trust Infrastructure for Emerging Payment Models	<u>28</u>
Additional Issue 3– Domestic Governance in a Global Payments Environment	<u>30</u>
Conclusion	<u>32</u>
References	<u>33</u>
Appendix A	<u>35</u>

Introduction

The payments industry is experiencing a fundamental shift in the way payment relationships are created, managed and executed.

Historically, many payment policy questions could be understood through the lens of individual payment rails and schemes. Today, however, technological developments are increasingly separating the functions of payment initiation, customer experience, authority management, orchestration and settlement. New participants are emerging across the payments value chain, while payment relationships are becoming increasingly digital, recurring, delegated and automated.

The amendments to the PSRA recognise that this changing environment may create new competition, efficiency and financial safety challenges that arise beyond traditional payment system boundaries. The reforms provide an opportunity to consider how payment system regulation can continue to support a competitive, innovative and resilient payments ecosystem as new technologies and business models emerge.

This submission focuses on a common theme that links many of the issues raised throughout the Review. Increasingly, some of the most important challenges facing the payments ecosystem relate not to the movement of value itself, but to the establishment and governance of trust.

As payments become more automated and interconnected, participants require confidence that payment authorities are valid, that consent can be evidenced, that liability can be assessed objectively, that payment relationships remain portable and interoperable, and that trust can be maintained across a diverse ecosystem of domestic and international participants. Industry may increasingly need to consider whether payment agreement creation, authority management, consent governance and evidence management are emerging as distinct infrastructure capabilities that operate across payment systems rather than within individual payment rails.

Historically, many of these functions have been embedded within individual payment systems and schemes. However, emerging payment models increasingly require these capabilities to operate consistently across multiple payment methods, technologies, providers and settlement environments.

This theme sits at the centre of many of the issues discussed throughout this submission and provides a useful lens through which to consider the future application of the amended PSRA.

This submission therefore proposes that the RBA consider how future payments regulation can support interoperable approaches to authority, consent, trust, governance and evidence management across payment systems. Such capabilities should remain technology-neutral, operate alongside existing payment system rules and liability frameworks, and support the continued development of competition, efficiency and financial safety within Australia's evolving payments ecosystem

Responses to Consultation Questions

Q6: Are there competition, efficiency and/or financial safety issues relating to the use of AI agents for payments in e-commerce? If so, are there any regulatory actions that the RBA should consider?

Yes.

The emergence of AI agents and agentic commerce has the potential to deliver significant consumer and merchant benefits. Consumers may increasingly choose to delegate elements of purchasing and payment decision-making to AI agents, creating more convenient and personalised commerce experiences. However, these developments also introduce new competition, efficiency and financial safety issues that are directly relevant to the objectives of the amended PSRA and the RBA's payments system mandate.

A key issue is the growing separation between payment authority and payment execution. This distinction is important because traditional payment frameworks were largely designed around a model in which the same party both authorised and initiated the payment.

Historically, consumers have directly initiated and authorised payments. In agentic commerce environments, authority may instead be delegated to software agents operating across multiple transactions, merchants and channels over an extended period. Participants throughout the payments ecosystem will therefore require reliable ways to evidence delegated authority and determine whether a transaction remains consistent with the permissions granted by the consumer.

Consumers would benefit from common approaches to authority and consent management that provide:

- clear visibility of what an AI agent has been authorised to do
- the ability to modify, suspend or revoke permissions
- transparency regarding how payment decisions are made
- reduced disputes relating to consumer intent
- greater confidence when adopting emerging technologies.

This is consistent with emerging research on agentic commerce, which suggests that consumer trust and adoption are strongly influenced by transparency, control and visibility of automated decision-making and payment activity.

The competition implications are equally significant. Many of the tools, protocols and operating environments emerging to support agentic commerce are being developed by global technology companies and international payment networks. Industry research increasingly anticipates that AI assistants, digital wallets and commerce orchestration platforms may become primary interfaces through which consumers interact with merchants and payment systems, increasing the importance of interoperability, portability and payment choice.

While these developments may deliver significant convenience benefits, they also create a risk that key control points within future payment ecosystems become concentrated within proprietary platforms. Unless interoperability, portability and payment choice are considered early, domestic participants may have limited ability to influence how payments are initiated, routed and governed.

Efficiency considerations also arise. AI agents may increasingly determine how payments are initiated and which payment methods are selected. Unless routing choice and interoperability are embedded from the outset, agentic commerce environments may reinforce existing limitations on competition between payment methods and payment rails, reducing the effectiveness of initiatives designed to promote merchant choice and payment system efficiency.

Financial safety considerations are similarly important. Australian payment service providers, acquirers, gateways and processors may increasingly receive payment instructions generated by AI agents without access to consistent and standardised evidence of the consumer's authority or intent. This creates uncertainty regarding the right to transact, increases dispute complexity and may result in higher operational, fraud and liability costs across the ecosystem. Without common approaches to evidencing delegated authority, participants may be required to make risk decisions using fragmented and proprietary information sets.

There is also a strong public interest case for early engagement. The RBA has noted that the development of agentic commerce use cases, rules and protocols is currently being led by international technology companies and payment networks. At the same time, evidence suggests that agentic commerce could scale rapidly as consumer trust and adoption increase.

This view is reinforced by evidence from mobile payment ecosystems, where strong network effects, platform concentration and switching costs have required increasing regulatory attention once adoption became established. International competition authorities have identified similar risks arising where critical payment interfaces become concentrated within a small number of technology providers.

Once network effects, commercial dependencies and consumer behaviours become established, competition and interoperability concerns become significantly more difficult and costly to address. The amended PSRA was specifically designed to support consideration of emerging risks before they become embedded within the payments system.

In this context, waiting until agentic commerce reaches scale is unlikely to produce the most effective policy outcomes. By that stage, market structures, technical architectures and commercial relationships may already be deeply entrenched. A proactive focus on interoperability, authority management and consumer protection is therefore consistent with both the intent of the PSRA reforms and the RBA's public interest mandate.

Recommended Regulatory Approach

Consistent with the objectives of the amended PSRA, the RBA should:

- prioritise understanding how authority, consent and liability will operate in agentic commerce environments
- support industry experimentation and pilot programs that test interoperable authority and consent frameworks
- encourage the development of portable and auditable permissioning models that operate independently of any individual payment rail, technology platform or provider
- promote interoperability, payment choice and merchant choice within agentic commerce payment flows
- ensure Australian payment institutions have access to objective evidence of delegated authority sufficient to support risk management, dispute resolution and liability allocation.

The RBA should not seek to regulate specific AI technologies or select winners amongst emerging agentic commerce participants. Rather, it should support industry-led development of interoperable trust, authority and governance frameworks that enable diverse participants to innovate and compete while ensuring emerging technologies remain aligned with Australian payments system objectives and support competition, efficiency and financial safety across the broader ecosystem.

Supporting industry-led exploration of interoperable authority, consent and governance frameworks would help ensure that emerging agentic commerce ecosystems remain aligned with Australian competition, efficiency, financial safety and consumer protection objectives as adoption grows.

Q11: What are the challenges faced by participants and end-users in the A2A payments system? Do these limit efficiency, competition or financial safety in relation to A2A transactions?

While clearing and settlement infrastructure remain important, many of the challenges emerging within the A2A ecosystem are increasingly occurring above the payment rail.

This is particularly evident for payer-not-present, recurring and ongoing payment arrangements, including direct debits, PayTo mandates and emerging authorised payment initiation models. In these use cases, the challenge is often not how funds move between institutions, but how payer authority, consent, permissions and liability can be consistently established, evidenced, maintained and relied upon over the lifecycle of the payment arrangement.

As the A2A ecosystem expands across multiple payment systems, initiation channels, digital wallets, software platforms, business systems and future agentic commerce environments, participants face increasing fragmentation in how consent and authority artefacts are created, stored, accessed and managed. This creates operational complexity for payment service providers, merchants and end-users, and can reduce transparency, efficiency and trust.

Key challenges include:

Fragmented consent and authority management

Consumers and businesses can establish ongoing payment commitments through multiple payment systems and channels, each with distinct mandate, consent and authority requirements. While these differences may be appropriate and necessary, there is limited consistency in how those artefacts are managed, accessed, updated, revoked or evidenced over time.

As a result, end-users often lack simple and consistent ways to understand, manage and control their ongoing payment commitments across providers and payment systems. This can reduce confidence and increase friction when adopting A2A payment services.

Operational complexity and manual processes

Participants frequently rely on fragmented operational processes when responding to disputes, claims, mandate enquiries, payment investigations and exception handling.

The lack of common approaches to participant identification, authority verification, mandate retrieval and lifecycle record management can increase operational costs and extend resolution timeframes. These inefficiencies become more pronounced as payment use cases become increasingly digital, automated and cross-platform.

Reduced transparency and trust

When authority information is fragmented across different systems and providers, participants may not have timely access to the information required to efficiently assess whether a payment was correctly authorised or operated within agreed permissions. This can create uncertainty during dispute resolution, increase the cost of managing exceptions and reduce confidence in newer payment models that rely on authorised third-party initiation or ongoing payment arrangements.

Barriers to interoperability and innovation

The A2A Vision ⁽²⁾ identifies interoperability, portability and appropriate standardisation as important characteristics of the future A2A ecosystem. However, today many consent and authority arrangements remain tied to individual payment products, channels or technology implementations rather than operating within a broader interoperable framework.

This can increase implementation costs, create duplicate infrastructure requirements and make it more difficult for participants to support new A2A payment experiences consistently across multiple payment systems.

Challenges associated with future payment models

The A2A Vision recognises that future payment arrangements may include digital identity, AI-enabled payment initiation, tokenised money, programmable transactions and alternative settlement models. These developments will increase the importance of being able to reliably establish, evidence and govern payer authority across diverse payment environments.

Without common approaches to authority governance and record management, future innovation risks introducing additional fragmentation and complexity into the ecosystem.

Supporting Evidence

While direct evidence relating specifically to Australian A2A recurring payment arrangements is limited, there is a substantial body of evidence from recurring payment, direct debit, card-on-file and subscription payment environments that highlights challenges relating to consent management, payment visibility, ongoing authority and dispute handling. Although some of this evidence originates from card payment ecosystems and overseas markets, many of the underlying dynamics are relevant to Australian A2A payment arrangements such as direct debit, PayTo and future authorised payment initiation models.

Importantly, most consumers and many small businesses do not distinguish between underlying payment rails when managing recurring payment obligations. Terms such as "direct debit", "automatic payment" and "subscription payment" are often used interchangeably to describe ongoing payer-not-present payment arrangements. As such, observed consumer behaviours and concerns in recurring payment environments are likely to provide useful insights into potential challenges facing the broader A2A ecosystem.

Consumer challenges managing ongoing payment commitments

International consumer protection bodies continue to receive complaints relating to recurring and ongoing payment arrangements, including situations where consumers: ^(6, 10)

- were unaware they had entered into a recurring payment arrangement
- experienced difficulty cancelling payment authorities
- were charged unexpectedly
- disputed the amount or frequency of payments
- continued to be charged following cancellation attempts.

The emergence of new subscription and auto-renewal consumer protection regimes in multiple jurisdictions, including Australia, reflects growing policy concern regarding consumer visibility, control and oversight of ongoing payment commitments. These reforms are designed to address "subscription trap" behaviours and improve transparency surrounding recurring payment arrangements. ^(4, 7, 8)

While consumer protection reforms are an important part of the solution, they do not address the full challenge. Regulatory changes can establish consumer rights and obligations, but the practical management of payment authorities, mandates and ongoing payment commitments remains a payments system issue. As jurisdictions such as Australia strengthen consumer protections relating to subscriptions and ongoing payment arrangements, there may be value in ensuring that payments infrastructure and governance frameworks support these policy objectives wherever possible. Doing so could help reduce operational complexity, improve compliance outcomes and avoid the creation of additional friction, duplication or inconsistency between consumer protection requirements and the mechanisms used to manage payment arrangements in practice.

Transaction confusion and authority visibility create disputes

Research published by Mastercard indicates that approximately 20 per cent of payment disputes were attributed to first-party fraud in 2025, while 48 per cent of consumers reported disputing at least one transaction that they later realised was legitimate. Mastercard attributes a significant portion of these disputes to transaction confusion, where consumers do not recognise or understand charges appearing in increasingly complex digital payment environments. ⁽⁹⁾

As payment initiation increasingly occurs through multiple channels, wallets, software platforms, subscription arrangements and automated processes, ensuring that payment authorities remain transparent, traceable and understandable becomes ever more important.

Disputes and operational complexity create system costs

The growth of first-party fraud and payment disputes is creating measurable operational costs across payment ecosystems.

The 2025 Global eCommerce Payments & Fraud Report found that 62 per cent of merchants reported increasing levels of friendly fraud and that first-party misuse is now among the fastest growing fraud categories.^(10, 11)

Similarly, the 2026 Chargeback Field Report⁽¹²⁾ found that:

- 83 per cent of enterprise merchants reported rising levels of friendly fraud
- 61 per cent reported increasing chargebacks
- 38 per cent indicated that dispute-related costs were being reflected in customer pricing.

While these findings relate primarily to card payment environments, they demonstrate how poor visibility of payment authority, transaction context and ongoing obligations can create material operational costs across participants.

Relevance to A2A payments

The future challenge for many recurring and payer-not-present A2A payment arrangements is increasingly not how value moves between accounts, but how authority, consent, permissions and trust are established, evidenced and governed throughout the lifecycle of the payment arrangement.

This observation is consistent with the industry's stated vision for A2A payments, which identifies identity verification, authority and consent management, mandate governance, interoperability, trust frameworks and payment lifecycle management as important future system characteristics. The A2A Vision further recognises that emerging technologies such as AI, digital identity, digital wallets and tokenised forms of money will increase the importance of these trust-layer functions over time.

Taken together, the available evidence suggests that fragmented approaches to authority management, consent governance, dispute handling and lifecycle record-keeping may create challenges for efficiency, competition and financial safety. These challenges are likely to become more pronounced as A2A payment arrangements expand into recurring, automated, delegated and programmable payment use cases. The resulting risks include increased operational costs, reduced consumer confidence, greater dispute complexity, barriers to interoperability and slower adoption of new payment capabilities.^(2, 5, 10)

This provides a reasonable basis for considering whether improved interoperability, transparency and governance of payment authorities and consent arrangements could support better outcomes for participants and end-users across the evolving A2A ecosystem.

Collectively, these challenges suggest that the future evolution of A2A payments may depend as much on the management of authority, consent and payment lifecycle information as it does on the efficiency of underlying clearing and settlement infrastructure.

Appendix A provides an example of an interoperable trust, authority and consent framework designed to operate alongside existing payment systems.

Q12: Is there a case for the RBA to take any regulatory action in relation to A2A payments to support efficiency, competition or financial safety, or control risk to the financial system? If so, what regulatory actions should be considered?

Yes.

The challenges identified in Question 11 suggest that some of the constraints on competition, efficiency and financial safety within the A2A ecosystem do not arise solely from clearing and settlement infrastructure. Increasingly, they arise from how payment authority, consent, permissions and mandates are established, evidenced, managed and relied upon across the lifecycle of recurring and payer-not-present payment arrangements. As A2A payment use cases continue to expand—including recurring payments, PayTo arrangements, digital wallets, authorised third-party payment initiation, embedded finance and future agentic commerce models—the ecosystem risks developing increasingly fragmented approaches to authority management, consent governance and record keeping. This may increase operational complexity, reduce transparency, create barriers to interoperability and increase the cost of dispute management for participants and end-users alike.^(2, 9, 9)

Importantly, this issue should not be viewed as a need to replace or harmonise the underlying consent requirements, rules or liability frameworks that exist within individual payment systems. Different payment systems appropriately maintain different authorisation, risk and liability requirements, reflecting the distinct characteristics of each payment type and use case.

Rather, there may be value in industry exploring whether payment-system-specific consent, authority and mandate requirements can be supported through a common governance and interoperability framework that improves how these artefacts are created, managed, accessed, evidenced and maintained throughout their lifecycle, whilst continuing to enforce and respect the requirements of each individual payment system.

Such an approach has the potential to reduce unnecessary duplication, improve portability, simplify operational processes and provide participants with more efficient ways to evidence authority and permissions without altering the underlying payment system rules themselves.

Recommended Regulatory Approach

Consistent with the objectives of the PSRA reforms and the RBA's mandate to promote competition, efficiency and financial safety, the RBA should support industry efforts to explore interoperable trust, authority and consent governance arrangements for recurring and payer-not-present payment typologies.

The RBA should:

- support industry experimentation and pilot programs that test interoperable authority, consent and mandate-governance frameworks
- encourage the development of portable and auditable approaches for managing payment-system-specific authority and consent artefacts across providers and payment environments
- promote interoperability, competition and merchant choice through common approaches to trust, authority, participant identification and lifecycle management
- encourage the development of standards and governance models that reduce operational complexity associated with disputes, claims, exception handling and ongoing payment management
- support approaches that remain technology-neutral and interoperable with future clearing and settlement innovations, including tokenised deposits, programmable money, digital identity ecosystems and other emerging forms of digital value.

This approach directly supports the outcomes sought by both the PSRA reforms and the emerging A2A Vision.

The A2A Vision identifies authority verification, mandate management, trust frameworks, interoperability, standardisation and future-readiness as important characteristics of Australia's future A2A ecosystem. It also recognises that emerging technologies such as AI, digital identity, digital wallets and tokenised forms of money will increasingly influence how payments are initiated, authorised and managed.

The A2A Payments Vision further notes that future A2A systems may require common trust frameworks, authority management capabilities and interoperability across different providers, platforms and forms of value.

Supporting industry exploration of these issues would therefore represent a proportionate and forward-looking response to challenges that are increasingly emerging above the payment rail itself. It would also help ensure that future innovation occurs within a framework that continues to support competition, efficiency, financial safety and consumer confidence, while avoiding unnecessary fragmentation or the creation of new barriers to participation.

Q14: What regulatory action, if any, should the RBA take to promote more standardisation and interoperability across cards and A2A payments?

While significant attention has been given to transaction speed, functionality, merchant acceptance and user experience, there may be other factors limiting effective competition and interoperability between card-based and A2A payment methods.

Many of these barriers occur above the transaction layer and relate to how payment relationships are established, managed and maintained over time. These include:

- differences in consent and authorisation frameworks
- differences in dispute and exception handling processes
- differences in ongoing authority and mandate management
- limited portability of payment relationships and recurring payment arrangements
- inconsistent consumer and merchant experiences across payment methods.

For many recurring and payer-not-present payment use cases, consumers and businesses are effectively managing an ongoing payment relationship rather than an individual transaction. Examples include subscriptions, memberships, utilities, recurring invoices, digital services and other ongoing payment arrangements.

When moving between payment methods today, consumers and businesses often need to:

- establish a new payment authority
- re-enter payment credentials or account details
- create a new mandate or payment instruction
- manage a separate cancellation, amendment and dispute process
- learn a new payment management experience.

This friction can discourage switching and reduce willingness to adopt alternative payment methods, even where those alternatives may offer efficiency, competition or cost benefits. As a result, competition outcomes may be influenced not only by the relative functionality of payment rails, but also by the ease with which consumers and merchants can move payment relationships between them.

Effective competition requires that consumers and businesses can move between payment options without losing visibility, control or continuity of their payment arrangements.

Portability as an interoperability issue

Promoting interoperability between cards and A2A payment systems should therefore extend beyond transaction messaging and payment execution.

There may be value in exploring how greater portability can be achieved for recurring and ongoing payment arrangements.

Greater portability could support:

- easier switching between payment methods
- reduced administrative burden for consumers and merchants
- lower migration costs
- increased willingness to adopt lower-cost payment options
- stronger competitive pressure between providers and payment methods.

Importantly, portability should not require the harmonisation or replacement of the underlying consent requirements, liability frameworks or scheme rules that apply within different payment systems. Different payment systems appropriately maintain different authorisation, risk and liability requirements.

Rather, industry may benefit from exploring whether payment-system-specific consent and authority artefacts can be captured, managed, maintained and evidenced through common standards and governance arrangements that support interoperability whilst continuing to enforce the requirements of each payment system.

This could provide a framework through which payment-system-specific authorities, mandates and permissions can be managed throughout their lifecycle while preserving the unique characteristics and protections of individual payment systems. This could improve portability and consistency without altering those protections.

Reducing fragmentation in recurring payment experiences

A related challenge is the growing fragmentation of payer-not-present payment experiences. Consumers increasingly interact with recurring and delegated payment arrangements through cards, direct debits, PayTo mandates, digital wallets and emerging digital commerce models. However, these arrangements are often managed through separate tools, interfaces and operational processes.

This fragmentation can reduce transparency, increase complexity and create inconsistent experiences for both consumers and businesses.

Exploring common approaches to the governance, management and lifecycle administration of recurring payment arrangements could help ensure that all payer-not-present payment models benefit from comparable levels of transparency, control, auditability and operational efficiency, regardless of the underlying payment rail.

Recommended Regulatory Approach

Consistent with the objectives of the amended PSRA, the RBA should:

- support industry experimentation and pilot programs that explore portability and interoperability of recurring payment relationships across payment systems
- encourage the development of common standards and governance arrangements for the lifecycle management of payment authorities and mandates
- support interoperable approaches to authority, consent and permission management which respect and preserve the requirements of individual payment systems
- promote interoperability that improves merchant and consumer choice without compromising safety or liability protections
- encourage industry to consider portability and trust-layer interoperability as part of broader card and A2A competition initiatives
- support approaches that remain compatible with future payment innovations, including tokenised deposits, programmable money, digital wallets and agentic commerce environments.

Alignment with the PSRA reforms and RBA objectives

The PSRA reforms recognise that competition, efficiency and safety outcomes increasingly depend on a broader range of participants, technologies and activities within the payments ecosystem, rather than solely on the operation of payment rails themselves. The RBA's stated objective is to promote competition, efficiency and financial safety across the payments system. Review of Payments System Regulation – Issues Paper also notes that a well-functioning payments system is characterised by contestability, interoperability and appropriate standardisation.

As payment relationships become increasingly digital, automated and long-lived, interoperability at the trust, authority and consent layer may become just as important as interoperability at the transaction layer. Supporting portability and reducing fragmentation in how payment relationships are managed could therefore improve competition between payment methods while delivering efficiency, consumer experience and innovation benefits across the broader payments ecosystem.

Q15: How is the payments industry strengthening its cryptographic practices in response to evolving cyber threats?

The payments industry is undertaking significant cryptographic uplift activity through both domestic and international initiatives. These efforts include migration to stronger encryption standards, the adoption of tokenisation, improvements to digital identity and authentication frameworks, increased use of hardware-backed security capabilities, development of post-quantum cryptography preparedness programs and broader cyber resilience investments.

These initiatives are essential and will continue to improve the security of payment credentials, communications and transaction processing. However, as payments become increasingly automated, recurring, delegated and embedded, the scope of cyber security challenges is also expanding.

For payer-not-present and ongoing payment arrangements, protecting payment credentials alone may no longer be sufficient. Cryptographic protection of payment authorities may be just as important as cryptographic protection of payment credentials.

There is also a growing need to protect the integrity of:

- payment authorities and mandates
- payer consent and permission parameters
- transaction instructions
- beneficiary and creditor information
- evidence used to support dispute resolution and liability assessment.

A future threat scenario may not involve theft of payment credentials, but rather the manipulation of payment permissions, payment terms or beneficiary details. In these circumstances, industry may increasingly require cryptographic methods that protect not only the payment transaction itself, but also the broader payment relationship and authority framework on which the transaction depends.

Most payment security programs historically focused on:

- card numbers
- account details
- transaction messages

Future payment ecosystems increasingly need to protect:

- who was authorised to act
- what they were authorised to do
- which terms were agreed
- whether those terms changed over time.

Emerging industry approaches are exploring the use of cryptographically signed agreement records, tokenised authority references and immutable event histories to ensure that payment agreements cannot be altered without detection and that payment participants can reliably verify both the existence and integrity of underlying payment authorities. This approach allows cryptographically verifiable authority information to travel alongside payment instructions, enabling participants to validate authority and permissioning relationships without requiring centralised lookups or reliance on less secure manual processes.

The same techniques may also improve the integrity of dispute and investigation processes. Rather than relying on the exchange of evidence through email or other fragmented processes, authorised parties could securely access cryptographically verifiable evidence and agreement records through permissioned interfaces. This may improve both security and operational efficiency.

Over time, cryptographically verifiable payment authority records may complement existing payment security controls by providing stronger assurance regarding the authenticity, integrity and provenance of recurring and payer-not-present payment arrangements.

A further benefit of focusing on cryptographic protections above the payment rail is that security methodologies can evolve over time without requiring disruptive changes to underlying clearing and settlement infrastructure. This allows industry to respond more rapidly to emerging threats, adopt new cryptographic standards as required and improve resilience while preserving investment in existing payment systems.

Q16: What key barriers or challenges are participants facing in uplifting cryptography and broader cyber security practices?

While progress is being made, several challenges may adversely affect industry-wide cryptographic uplift initiatives.

Coordination across a diverse ecosystem

Payments involve a broad range of participants including financial institutions, PSPs, payment schemes, merchants, software providers, digital identity providers and technology platforms. While individual organisations can strengthen their own cryptographic controls, achieving broader ecosystem benefits often requires coordinated adoption and interoperability between participants.

Historically, many industry security initiatives have been organised on a payment-system-by-payment-system basis, reflecting the structure of Australia's payment rails and schemes. However, some of the emerging cyber security and integrity challenges associated with recurring, delegated and payer-not-present payment arrangements are increasingly independent of any single payment rail.

For example, protecting the integrity of payment authorities, consent parameters, payer permissions, recurring mandates and payment agreement records is relevant across a broad range of payment types, including direct debit, PayTo, card-on-file transactions, digital wallet initiated payments and emerging agentic commerce models. These challenges relate to the creation, management and governance of payment agreements rather than the movement of funds through any individual payment system.

As a result, cryptographic approaches such as agreement tokenisation, signed authority records, immutable event histories and secure permissioned access to payment evidence may require coordination across multiple payment systems and participants. This creates a challenge for industry because responsibility for these capabilities does not naturally sit within any single payment rail or scheme governance structure.

The industry therefore faces a coordination challenge in determining whether payment agreement creation, authority management and consent governance should increasingly be treated as distinct components of payments infrastructure, operating alongside settlement and processing systems rather than being embedded independently within each payment rail.

Lack of common approaches above the payment rail

Many cyber security investments today focus on protecting payment credentials and transaction messaging within individual payment systems.

However, emerging payment models increasingly rely on shared authority, consent, identity and mandate information that spans multiple providers, channels and payment systems.

The absence of common approaches to securing these artefacts can create fragmentation and reduce the effectiveness of security investments.

Operational and economic challenges

Cyber security improvements often require sustained investment and collaboration despite benefits being distributed across multiple participants.

Where ecosystem-level benefits exist, industry may need greater coordination and stronger signals regarding future direction, standards and policy priorities.

Q17: What role could the RBA play in supporting and coordinating industry-wide cryptographic uplifts in the payments system, while avoiding both duplication and undermining existing domestic and international standards, regulatory frameworks or industry-led initiatives?

The RBA has an important role in supporting industry-wide cryptographic uplift while avoiding duplication of existing domestic and international regulatory, standards and industry-led initiatives.

Rather than prescribing specific technologies or cryptographic implementations, the RBA could help establish the conditions under which industry can safely experiment, collaborate and develop interoperable approaches to emerging security challenges.

The amended PSRA recognises that competition, efficiency and financial safety issues increasingly arise across a broader set of participants and activities than traditional payment system operators alone. The RBA is therefore uniquely positioned to support industry coordination on issues that cut across multiple payment systems and to provide clear signals where payment agreement creation, authority management and consent governance are emerging as distinct infrastructure capabilities that operate across, rather than within, individual payment systems.

In particular, the RBA could:

- support industry experimentation and proof-of-concept activities focused on cryptographically verifiable payment authority and consent management
- support and endorse an industry coordination body, such as AusPayNet, to facilitate industry experimentation, proof-of-concept activities and stakeholder collaboration on cross-system approaches to authority management, consent governance and cryptographic trust frameworks
- encourage exploration of secure and interoperable approaches to agreement tokenisation, digital signatures and permissioned access to payment-related evidence
- promote collaboration between payment participants, standards bodies and cyber security specialists to ensure emerging approaches remain compatible with existing payment system requirements
- encourage the development of approaches that operate independently of any individual payment rail and can therefore support multiple payment systems and future settlement models
- facilitate evidence gathering regarding the effectiveness, costs and benefits of emerging cryptographic approaches before any regulatory intervention is contemplated.

Industry experimentation may also help determine how cryptographic protections can be extended beyond payment credentials and transaction messages to encompass authority, consent and payment agreement frameworks. Such capabilities may strengthen protection against tampering, improve the integrity of payment lifecycle records and support more efficient dispute and investigation processes.

The preferred approach is to regulate outcomes and risks while allowing industry participants flexibility in how interoperability is achieved. Emerging industry-led frameworks demonstrate how trust, authority and consent management may be delivered across multiple payment systems without requiring changes to underlying payment rails (see Appendix A).

Supporting exploration of these concepts would be consistent with the objectives of the PSRA reforms. As payments become increasingly automated, recurring and interoperable, cryptographic protections may need to extend beyond transaction processing into areas such as authority management, consent governance, dispute handling and evidence integrity.

Such an approach would support competition, efficiency and financial safety by improving trust, reducing opportunities for tampering, strengthening auditability and creating a foundation upon which future payment innovations—including tokenised and programmable forms of money—can operate securely.

Q19: Are there any other issues relating to payments that the RBA should consider prioritising to promote competition, efficiency and financial safety in the payments system? Are there regulatory options outside of the RBA's formal powers under the PSRA to address the issues outlined in this paper? Are there issues in the broader payments system that have implications for the design and implementation of the RBA's payments system regulation?

Cross-System Issues Beyond Individual Payment Rails

While many of the issues raised throughout this submission relate to specific payment methods or emerging technologies, a recurring theme is that some of the most significant future challenges do not naturally sit within any one payment rail, scheme or participant group. Increasingly, issues such as payment authority governance, dispute evidence integrity, consent lifecycle management, cryptographic protection of payment arrangements and trust-layer interoperability operate across multiple payment systems simultaneously. These issues may therefore benefit from industry-wide coordination that extends beyond the governance structures of individual payment systems.

In addition to its formal powers under the PSRA, the RBA may be well positioned to use its convening role to support collaboration on these broader ecosystem challenges. Such work could complement existing regulatory frameworks without requiring prescriptive intervention and may assist the industry in achieving broader public interest outcomes relating to trust, efficiency, cyber resilience, competition and interoperability.

Against this backdrop, the following three issues are highlighted because they demonstrate how important payment system outcomes are increasingly shaped by trust, authority, governance and interoperability capabilities that cut across multiple payment rails, participant groups and technology environments.

Additional Issue 1 – First-party fraud, dispute efficiency and authority verification

An issue that may warrant further consideration is the increasing operational and economic impact of first-party fraud and payment disputes across the payments ecosystem.

While existing liability and dispute frameworks play a critical role in maintaining consumer confidence and protecting end-users from genuine harm, there is increasing evidence that a growing proportion of disputes relate not to unauthorised transactions, but to situations where consumers do not recognise, recall or accept responsibility for transactions that were in fact initiated or authorised.

Research published by Mastercard ⁽⁹⁾ indicates that approximately 20 per cent of disputes were attributable to first-party fraud in 2025, while 48 per cent of consumers reported disputing at least one transaction that they later realised was legitimate. Mastercard attributes a significant proportion of these outcomes to transaction confusion and an inability to easily identify or understand charges within increasingly complex digital payment environments.

Similarly, the 2025 Global eCommerce Payments & Fraud Report ⁽¹³⁾ found that 62 per cent of merchants reported increasing levels of first-party misuse, while the 2026 Chargeback Field Report ⁽¹²⁾ found that 83 per cent of enterprise merchants had experienced growth in friendly fraud and that dispute-related costs were increasingly being reflected in customer pricing. Although much of the available evidence originates from card-based payment environments, many of the underlying dynamics are equally relevant to recurring and payer-not-present payment arrangements more broadly. Importantly, most consumers and many small businesses do not distinguish between underlying payment rails when managing ongoing payment obligations. Direct debits, card-on-file subscriptions, recurring wallet payments, PayTo arrangements and emerging payment initiation models are often perceived simply as ongoing or automatic payments.

The challenge is increasingly not determining whether funds moved correctly, but determining whether the authority, permissions and obligations sitting behind a payment can be evidenced efficiently, objectively and with confidence.

An emerging consideration is how the payments ecosystem will efficiently support an expanding range of consumer protection, reimbursement and dispute obligations. Existing payment scheme liability settings, proposed reimbursement mechanisms under the Scams Prevention Framework ⁽³⁾, and recent reforms addressing subscription traps and recurring payment arrangements – such as the recent update to the Australian Consumer Law ⁽⁴⁾ are all intended to strengthen consumer protection and confidence.

However, as these protections evolve, there may be a growing need for efficient, objective and immutable evidence of authority, intent and payment obligations to ensure that protections are applied fairly and consistently.

Without such capabilities, participants may face increasing operational complexity when distinguishing genuine consumer harm from transaction confusion, disputed authority or potential misuse of reimbursement and dispute processes. Payment system architecture should therefore seek to support emerging policy objectives by providing secure and auditable mechanisms for evidencing payment authorities and permissions, helping stakeholders comply with evolving obligations while reducing friction, duplication and opportunities for exploitation.

This issue may become more important as payment systems evolve and new payment models emerge. For recurring and payer-not-present payment arrangements, participants are increasingly required to evidence authority, permissions and payment rights throughout the lifecycle of a payment relationship. Without effective mechanisms for evidencing these rights and obligations, dispute resolution can become costly, fragmented and dependent on manual investigation.

Industry may therefore benefit from exploring rail-agnostic approaches that improve the integrity, accessibility and auditability of payment authorities and payment lifecycle records. Emerging approaches are demonstrating how cryptographically protected authority records, tokenised references, digitally verifiable permissions and immutable event histories may provide objective evidence of the existence, status and integrity of payment arrangements. Such capabilities have the potential to improve transparency, reduce operational complexity, strengthen dispute handling and support more effective implementation of liability frameworks without altering the underlying rules or protections of individual payment systems.

This issue sits at the intersection of competition, efficiency and financial safety.

More transparent and objective approaches to authority verification may improve consumer confidence, reduce operational costs associated with disputes and support innovation in recurring, delegated and payer-not-present payment models. Industry may therefore benefit from considering whether authority management and dispute evidence capabilities should increasingly be viewed as cross-system infrastructure functions rather than payment-system-specific functions.

Additional Issue 2 – Trust Infrastructure for Emerging Payment Models

A broader issue that may warrant consideration is how Australia can ensure that its payments architecture remains adaptable to emerging payment models, including tokenised deposits, programmable money, digital representations of value and other forms of digitally native payment instruments.

While there remains uncertainty regarding the timing, adoption and ultimate form of these technologies, many emerging models share a common requirement for trusted mechanisms relating to:

- participant accreditation and trust management
- authority verification
- access control and permissioning
- consent and mandate governance
- auditability and evidencing of payment rights and obligations.

These capabilities are likely to remain important irrespective of the underlying settlement mechanism or payment rail utilised.

Historically, new payment models have often required participants to recreate trust arrangements, onboarding processes, authority controls and governance frameworks for each new technology. This can increase complexity, create barriers to adoption and potentially lead to unnecessary concentration of control within particular platforms or ecosystems.

There may therefore be value in considering whether certain trust and governance capabilities should be designed as reusable components of Australia's broader payments architecture rather than being rebuilt separately within each new payment system or technology environment.

A consistent and interoperable approach to participant accreditation, authority verification, access control and consent governance could allow future payment innovations to emerge and compete on their merits while ensuring appropriate stakeholder protections are maintained. Such an approach may also reduce implementation costs, improve interoperability and support competition by avoiding unnecessary duplication across payment systems and technology providers.

Importantly, this should not require the harmonisation of payment system rules or the centralisation of payment system operation. Rather, the objective should be to establish clear and interoperable governance foundations that enable market-led innovation to occur within a framework that supports trust, efficiency, competition and financial safety.

From a public policy perspective, the opportunity is not simply to prepare for a particular future technology, but to ensure that the Australian payments ecosystem is capable of adapting as technologies evolve.

In this context, the RBA may wish to consider whether future payments regulation should continue to support the development of technology-neutral trust and governance capabilities that operate across payment systems and settlement models.

Such capabilities could help ensure that emerging payment innovations can be adopted to the benefit of consumers, businesses and payment providers while preserving competition, avoiding unnecessary concentration and maintaining confidence in the payments system.

As payment systems continue to evolve, Australia should seek to ensure that trust, authority, permissioning and governance frameworks are capable of evolving independently of the underlying settlement infrastructure. This will allow new payment models to be adopted more efficiently, reduce fragmentation across the ecosystem and provide a durable foundation for innovation while preserving competition, efficiency and stakeholder protections.

Additional Issue 3– Domestic Governance in a Global Payments Environment

A broader issue that may warrant consideration is how Australian payment policy objectives can continue to be reflected in payment ecosystems that are increasingly influenced, orchestrated or controlled by global technology providers.

Historically, payment systems, governance arrangements and participant obligations were closely aligned. However, technological developments are increasingly separating payment initiation, customer experience, payment orchestration and settlement into distinct layers. As a result, participants that play a significant role in how payments are initiated and managed may increasingly sit outside traditional payment system governance structures and, in some cases, outside the practical reach of domestic regulation.

This does not diminish the importance of regulation, standards or policy settings. Rather, it highlights that regulation alone may not always be sufficient to ensure domestic objectives relating to competition, consumer protection, efficiency and financial safety are reflected in future payment environments.

Australia may therefore benefit from considering whether certain trust, governance and interoperability capabilities should be embedded within domestic payments architecture itself. Such capabilities could help ensure that participants operating within Australian payment ecosystems are able to interact in ways that are consistent with domestic policy settings regardless of where technology providers are located or how payment initiation services evolve. Australia may therefore benefit from considering whether certain trust, governance and interoperability capabilities should be embedded within domestic payments architecture itself.

Such capabilities could help ensure that participants operating within Australian payment ecosystems are able to interact in ways that are consistent with domestic policy settings regardless of where technology providers are located or how payment initiation services evolve.

Importantly, the objective should not be to centralise payment system operation or restrict innovation. Rather, the objective should be to establish a clear and interoperable framework within which market participants can continue to innovate, compete and introduce new technologies while maintaining appropriate protections for consumers, merchants and payment providers.

This may become increasingly important as the industry explores future payment models including tokenised deposits, programmable money, AI-enabled payments, digital identity ecosystems and other emerging forms of digital value. In the absence of common governance and interoperability foundations, there is a risk that participants develop fragmented, duplicative or incompatible approaches that increase operational costs, reduce portability and create new barriers to competition.

Conversely, establishing common and technology-neutral governance foundations could support a more coordinated and efficient industry response to future innovation. It would allow new participants and technologies to compete on their merits while reducing unnecessary duplication of trust, permissioning and governance functions across the ecosystem.

From a public policy perspective, the objective should be to ensure that the adoption of globally driven technologies does not inadvertently weaken domestic competition, consumer protection, resilience or payments policy outcomes. A framework that enables global participants to operate within consistent domestic trust and governance settings may help preserve these objectives while still allowing the Australian market to benefit from rapid technological innovation.

Such an approach could strengthen domestic resilience, support competition, reduce fragmentation and create a durable foundation for future innovation while preserving the flexibility of market-led technology adoption.

Conclusion

The payments ecosystem is entering a period in which innovation will be defined not only by new payment rails and settlement models, but by new ways in which payment relationships are established, authorised, governed and trusted.

The issues considered throughout this submission—agentic commerce, A2A adoption, payment portability, cyber security, first-party fraud, tokenised money and global payment platforms—may appear distinct. However, they share a common underlying theme. Increasingly, competition, efficiency and financial safety outcomes are being determined by how trust, authority, consent, permissioning and evidence are managed across the payments ecosystem.

The PSRA reforms recognise that important payment functions increasingly occur above payment rails, across payment systems and through intermediaries. This creates an opportunity for the RBA to take a broader view of the infrastructure required to support a modern, competitive and resilient payments ecosystem.

The submission does not advocate for the replacement of existing payment system rules, liability frameworks or settlement infrastructure. Rather, it proposes that Australia explore whether interoperable trust, authority and governance capabilities can complement existing payment systems by reducing fragmentation, improving portability, strengthening cyber resilience and supporting innovation across multiple payment models.

Importantly, this is not simply a question of responding to current market developments. It is a question of ensuring that Australia remains prepared for future ones. Technology, payment methods and market structures will continue to evolve. The trust, governance and interoperability foundations that support them should be capable of evolving as well.

The public interest opportunity presented by the PSRA reforms is therefore not only to respond to emerging risks, but to establish the foundational conditions for future innovation.

Australia has an opportunity to ensure that trust, authority, consent, interoperability and governance can evolve independently of any particular payment rail, technology provider or settlement model. If successful, this will help ensure that future payment innovation strengthens competition, efficiency and financial safety rather than creating new forms of fragmentation, concentration or operational complexity. In doing so, the RBA can help position Australia as an active participant in the design of future payment ecosystems rather than a passive adopter of technologies developed elsewhere.

References

1. Reserve Bank of Australia (RBA)

Title: Review of Payments System Regulation – Issues Paper

Publisher: Reserve Bank of Australia

URL: <https://www.rba.gov.au/payments-and-infrastructure/regulatory-reviews/review-of-payments-system-regulation-2026/2026-06/>

2. A2A Payments Vision

Title: A2A Payments Vision

Publisher: Australian payments industry / AusPayNet and industry participants

URL: <https://a2apaymentsaustralia.com.au/wp-content/uploads/2026/07/a2a-payments-vision.pdf>

3. Australian Treasury

Title: Scams Prevention Framework – Draft Law Package and Position Paper

Publisher: Australian Treasury

Date: November 2025

URL: <https://beta.treasury.gov.au/key-activities/consultations/c2025-715201>

4. Australian Government Treasury

Title: Government Targets Hidden Fees and Subscription Traps in Crackdown on Unfair Trading Practices

Publisher: Australian Treasury

Date: 9 February 2026

URL: <https://ministers.treasury.gov.au/ministers/andrew-leigh-2025/media-releases/government-targets-hidden-fees-and-subscription-traps>

5. Mastercard

Title: Publications relating to Agent Pay, AI Commerce and Digital Trust

Publisher: Mastercard

URL: <https://www.mastercard.com/news>

6. Financial Ombudsman Service (United Kingdom)

Title: Regular Payments: Complaints We Can Help With

Publisher: Financial Ombudsman Service

URL: <https://www.financial-ombudsman.org.uk/consumers/complaints-can-help/banking-and-payments/regular-payments>

7. Stephenson Solicitors

Title: New UK Consumer Protection Regulations for Subscription Contracts

Publisher: Stephenson Solicitors

URL: <https://www.stephensons.co.uk/site/blog/commercial-blog/new-uk-consumer-protection-regulations-for-subscription-contract>

8. MSR Solicitors

Title: Auto-Renewals and Subscription Traps: What UK Businesses Need to Know in 2025

Publisher: MSR Solicitors

URL: <https://www.msrs.co.uk/auto-renewals-and-subscription-traps-what-uk-businesses-need-to-know-in-2025/>

9. Mastercard

Title: First-Party Fraud: Why Is It So Hard to Tackle?

Publisher: Mastercard

URL: <https://www.mastercard.com/us/en/news-and-trends/Insights/2024/first-party-fraud-why-is-it-so-hard-to-tackle.html>

10. Visa Acceptance Solutions

Title: 2025 Global eCommerce Payments & Fraud Report

Publisher: Visa Acceptance Solutions (formerly Cybersource)

URL: <https://www.visaacceptance.com/content/dam/documents/campaign/fraud-report/global-fraud-report-2025.pdf>

11. Verifi (A Visa Solution)

Title: 2025 Fraud and Payments Report

Publisher: Verifi

URL: <https://www.verifi.com/2025-fraud-and-payments-report.html>

12. Chargebacks911

Title: 2026 Chargeback Field Report

Publisher: Chargebacks911

URL: <https://chargebacks911.com/chargeback-field-report/>

An example of an Industry-Led Trust and Authority Framework

One example of an industry initiative exploring themes discussed throughout this submission is the **Interoperable Payment Agreement Framework** (IPAF). IPAF is being explored through industry engagement and proof-of-concept activities as a potential approach to improving the creation, management, portability and evidencing of payment authorities across multiple payment systems.

IPAF is not a payment rail, payment scheme or settlement mechanism. Rather, it is designed as a technology-neutral governance and interoperability layer intended to operate alongside existing payment infrastructure.

The framework explores whether payment authorities, mandates, permissions and consent artefacts can be managed through common governance arrangements while preserving the underlying rules, liability models and operating requirements of individual payment systems.

The framework is based on several core concepts:

- creation of a durable and auditable record of payment authority
- cryptographically verifiable evidence of consent and agreement lifecycle events
- portability of payment relationships across payment methods and providers
- interoperability across card, account-to-account and future payment systems
- privacy-preserving architecture that does not require personal information to be transmitted within payment transactions
- permissioned access to authority and evidentiary information for authorised participants.

The framework is intended to address challenges that increasingly arise above the payment rail, including recurring and payer-not-present payments, authority verification, dispute investigation, consent management, delegated payment models and future agentic commerce use cases. It also seeks to provide a framework through which emerging payment models, including tokenised forms of value, could operate within consistent trust and governance arrangements.

Importantly, IPAF does not seek to replace existing payment systems or liability frameworks. Instead, it explores whether common approaches to authority management, evidencing and governance could reduce fragmentation, improve portability, strengthen competition and support more efficient dispute resolution while allowing individual payment systems to continue operating under their existing rules.

Industry Proof of Concept

An industry proof of concept is being explored to test these concepts across existing payment infrastructure.

The objective is to evaluate whether a common authority and trust framework could support broader policy objectives relating to competition, efficiency, interoperability, cyber resilience and financial safety without requiring material changes to existing payment systems.

The proof of concept is intended to generate evidence and practical insights that would assist industry and regulators in considering whether such approaches warrant further exploration.

IPAF is included as a practical example of how interoperable trust, authority and governance capabilities could be implemented alongside existing payment systems to address many of the challenges identified throughout this submission.