21 August 2026

Head of Payments Policy Department
Reserve Bank of Australia
GPO Box 3947
Sydney NSW 2001

Australian Payments Network
Connect Inspire Thrive

By email only: pysubmissions@rba.gov.au

Australian Payments Network (AusPayNet) welcomes the opportunity to respond to the Issues Paper for the Reserve Bank of Australia's (RBA) Review of Payments System Regulation (the Review).

AusPayNet is the industry association and self-regulatory body for the Australian payments industry. We manage and develop standards and guidelines governing payments in Australia. Our purpose is to create confidence in payments by: setting enforceable industry standards for a safe, reliable and effective payments system; leading transformation in payments to drive efficiency, innovation and choice; and being the home for ecosystem collaboration and strategic insight. AusPayNet currently has more than 160 members including financial institutions, payment system operators, major retailers and financial technology companies.

This submission has been prepared by AusPayNet Management. It reflects AusPayNet's independent assessment of the issues raised by the Issues Paper from an industry-wide perspective and does not seek to present a consensus view of AusPayNet's members. Given the breadth and diversity of AusPayNet's membership, different member cohorts may hold differing views on particular issues, reflecting their respective roles in the payments ecosystem. Those perspectives will be detailed in members' individual submissions to the RBA. AusPayNet's submission focuses on the system-wide considerations that should inform the RBA's prioritisation of issues and assessment of potential regulatory responses.

Executive Summary

The payments value chain has expanded significantly over the past decade, as new technologies, business models and intermediaries have changed how payments are initiated, processed and experienced. These developments have delivered substantial benefits for consumers and businesses, while making the payments ecosystem more functionally diverse and interconnected. AusPayNet therefore welcomes the amendments to the *Payment Systems (Regulation) Act 1998* (PSRA) and the RBA's Review as an important opportunity to assess this contemporary payments ecosystem within a coherent regulatory framework.

The breadth of the Review is a natural consequence of the expanded regulatory perimeter and the number of activities that have not previously been subject to detailed examination. Consistent with the prioritisation focus of the Issues Paper, AusPayNet considers that the central task of this Review is to distinguish matters warranting early regulatory attention from those requiring further evidence, continued monitoring, or time for existing initiatives to progress. The RBA's expanded information-gathering powers should provide a stronger basis for assessing the nature and materiality of potential concerns, the roles of the relevant entities, and the sufficiency of existing responses. In making those assessments, we encourage the RBA to take a broad view of efficiency that encompasses quality, security, reliability and innovation as well as cost, and to favour targeted, proportionate responses that build on effective industry arrangements wherever possible. Timing should reflect the circumstances of each issue, with some matters requiring earlier certainty, while others should allow current industry work and evidence-gathering to progress. This differentiated approach would enable the RBA to direct its expanded powers towards the matters where they can deliver the greatest public interest benefit while preserving the industry's capacity to implement change safely and effectively.

Against this background, AusPayNet has set out our principal positions on many of the policy matters raised in the Issues Paper:

- **Merchant choice and competition:** Effective merchant choice requires both credible alternatives and the practical ability to act on them. If the Review confirms that material impediments to token portability remain, targeted formalisation of the RBA's existing expectations may be appropriate, building on the technical arrangements already established. In contrast, we do not support treating payment service integration and bundling as a systemic problem; any competition concerns raised that involve specific platforms should be assessed case-by-case by the appropriate regulator.
- **Account-to-account (A2A) payments:** AusPayNet supports the continued modernisation of A2A payments through the coordinated development of the A2A Payments Vision and Roadmap through the A2A Roundtable, in which the RBA is participating. While some outcomes may require regulatory support, that need should be established through the Roadmap development process. The RBA should defer setting priorities or reaching conclusions on A2A matters until the Roadmap is complete.
- **Mobile payments:** While mobile wallets have delivered substantial competition and efficiency benefits, longstanding uncertainty remains around effective access, issuer fees, and related conduct. Resolving whether current arrangements create material competition or efficiency concerns should be a priority outcome of this Review. The RBA and Australian Competition and Consumer Commission (ACCC) should coordinate a detailed assessment and, if material concerns are established, consider a targeted response that preserves security and investment incentives.
- **Agentic commerce:** Agentic commerce development remains at an early stage, and current evidence does not support regulatory intervention at this time. The RBA should monitor adoption and emerging standards, engage with relevant industry work, and allow market and industry-led arrangements to develop before considering any prescriptive requirements.
- **Cryptography and security:** Strengthening cryptographic protection across payments is a critical initiative requiring early and coordinated action. The RBA should support this work through a co-regulatory model that establishes an enforceable cryptography standard for all critical payment systems, while building on the technical and implementation foundations established by industry. This work should begin ahead of the Review's final conclusions, and be supported by coordinated readiness assessments for systems outside of the existing card migration program.
- **Overseas card payments fraud:** While overseas card-not-present (CNP) fraud is an important safety and efficiency issue, ongoing issuer, scheme and coordinated industry work is the most appropriate near-term response. The RBA should allow this work to progress before considering formal action, with AusPayNet keeping it informed as the evidence base and industry response mature.

These positions and the regulatory principles that underpin them are detailed in the remainder of our submission.

Regulatory Principles & Approach

Beyond considering a broader range of payments ecosystem participants, the Review also provides an opportunity for the RBA to consider how its regulatory principles should be applied effectively across a wider and more functionally diverse ecosystem.[1] This section outlines several important considerations that we consider should inform its assessment of potential policy responses, and that underpin AusPayNet's positions on the issues addressed in our submission.

Efficiency

As noted in AusPayNet's submission to the Issues Paper for the RBA's Review of Merchant Card Payment Costs and Surcharging (MCPCS Review), AusPayNet members have raised concerns about the RBA's focus on end-user costs as a primary measure of efficiency and competition in the payments ecosystem. While we agree that competitive pressure driving down prices is an important indicator of system efficiency, the RBA's own framework recognises three dimensions of efficiency – technical, allocative, and dynamic.[2] Together, these dimensions encompass matters such as the quality, security, reliability and functionality of payment services, whether resources are directed towards the services that provide the greatest overall benefit, and the capacity of the ecosystem to innovate and adapt as technology, risks and user needs change.

These broader aspects of efficiency are evident in the Australian payments ecosystem today. For example, the operational reliability of Australia's payments infrastructure and the increasingly sophisticated fraud-prevention capabilities that allow end-users to transact with confidence while protecting them from evolving threats reflect both technical and dynamic efficiency. Dynamic efficiency can also be seen in the continuing evolution of Australia's payments system to support new forms of commerce and to meet changing user expectations and technology preferences. Maintaining this adaptability requires ongoing investment in new technologies and capabilities, even where that may increase certain costs.

Regulatory interventions focused primarily on cost should therefore be carefully evaluated against their potential impact on the broader aspects of efficiency. A change that reduces one component of merchant payment costs may not produce a net efficiency gain for merchants over time if it ultimately diminishes technical or dynamic efficiency. The RBA should therefore take a holistic view that considers costs alongside quality, security, innovation and the long-term sustainability of the payments system, as well as how the costs and benefits are distributed across relevant stakeholders over time.

Competition

AusPayNet agrees with the RBA that effective competition is central to a well-functioning payments system. Australia's payments ecosystem demonstrates substantial competition across providers, business models, and payment propositions, supported by continuing innovation. In considering potential concerns, the focus should be on whether providers can enter and expand, offer viable and differentiated propositions, and exert competitive discipline through credible alternatives on which users can act. Effective competition does not require every payment service, rail or capability to be

---

1 The RBA signalled its intention to seek feedback as part of this Review on whether the key principles it uses to determine when regulatory intervention may be justified remain appropriate and are being applied effectively in a speech: Connolly, E (2024), *Online Retail Payments – Some Policy Issues*, Speech at the Merchant Risk Council Conference, 18 June.

2 RBA, *Payments System Regulation: Approach to Regulation*, accessed August 2026.

available through every provider or interface, or the number of options to be maximised irrespective of their value to users.

Constraints may nevertheless arise where access to shared infrastructure, a material interface or another difficult-to-bypass gateway is necessary for otherwise viable competition. Interoperability, standardisation or access arrangements can support competition in these circumstances by reducing barriers to entry, expansion, or switching. Any such measures should be calibrated to the identified constraint, while still preserving legitimate incentives for differentiation, investment, and innovation, including at the common layer. Scale, integration and service bundling, for example, are not, by themselves, evidence of a competition problem. Their effects should be assessed in context, including whether they involve control of a material gateway, create durable barriers to entry, expansion or switching, and the practical alternatives available to users and competitors.

Evidence-based and proportionate regulatory responses

The expanded information-gathering powers are an important immediate benefit of the PSRA reforms. They enable the RBA to investigate potential public-interest concerns across a much broader set of participants and functions, and should significantly strengthen the foundations for any policy decisions, by helping to more precisely establish the nature and materiality of any concern, the entities involved in causing or addressing it, and the sufficiency of industry responses.

The resulting evidence should inform both whether to regulate and the design of any response. AusPayNet has long supported technology-neutral regulation based on the principle of 'same activity, same risk, same rules'. However, entities contributing to the same broader product or service do not necessarily perform the same activity, create the same risks, or have the same ability to cause or address an identified issue. Regulatory responses should therefore be directed to the relevant entities and functions, while accounting for indirect costs, legitimate differences between payment propositions and business models, security and resilience implications, implementation feasibility, and legitimate commercial sensitivity concerns.

Transparency illustrates the importance of tailoring regulatory measures to their intended outcome. As detailed in our submission to the MCPCS Review, public disclosure can support competition, efficiency, accountability and compliance, but only where the intended users can understand the information and act on it. It may have limited effect where users lack credible alternatives or bargaining power, or where disclosure does not remove the underlying constraint; raw pricing comparisons may also obscure important differences in functionality, service and safety. In some cases, confidential reporting to the RBA could provide the necessary visibility with a lower regulatory impact, and without exposing commercially sensitive information. Disclosure requirements should therefore reflect their intended audience, the decisions available to them, and whether a more direct or complementary response is required.

Regulation and industry self-regulation

AusPayNet supports the RBA's longstanding presumption in favour of industry self-regulation, with regulatory intervention occurring only where the industry is unable to address a public interest concern. This approach recognises that industry participants often have strong incentives and the operational expertise to maintain trust, security, reliability and service quality, and to adapt arrangements as technology and risks evolve. As the industry's self-regulatory body, AusPayNet supports this work by leading a range of industry transformation and standards-setting initiatives, with a particular focus on infrastructure modernisation, interoperability, security and resilience. The industry-led approach has delivered continued innovation, major infrastructure developments, and comprehensive security and risk management frameworks, demonstrating that self-regulatory approaches can support efficiency and help deliver policy objectives without prescriptive mandates.

The appropriate balance between regulatory and industry-led action depends on the extent to which existing industry arrangements can independently deliver the required outcomes. The industry's proactive approach to addressing many competition, efficiency and safety issues has meant that the RBA has imposed regulation in a relatively narrow range of payments system activity to date. As the payments ecosystem becomes increasingly complex and disintermediated, however, industry arrangements may not always be able to reach every entity whose participation is necessary to deliver a market-wide outcome. Targeted formal regulation or co-regulation may therefore become more important for ensuring broad coverage, enforceability, independent oversight, and timely and consistent implementation across the payments value chain. Co-regulation can be particularly effective by providing an appropriate backstop while allowing the industry to develop the technical and operational arrangements that best deliver the required outcome.

Prioritisation and sequencing

The breadth of this Review is a natural consequence of the RBA's expanded remit under the PSRA, and the number of payments system activities that have not previously been subject to detailed examination. The Review's prioritisation exercise should determine not only which matters warrant active regulatory work, but also the appropriate pathway and timing for each. This should reflect the materiality and urgency of each issue, the cost of delay, dependencies with other initiatives, and the cumulative volume of regulatory, technological and infrastructure change across the payments ecosystem.

The industry is simultaneously implementing a number of major regulatory reforms – including the Review of Merchant Card Payment Costs and Surcharging, the PSP licensing framework, and the Scams Prevention Framework – modernising A2A payments, and undertaking major security and resilience uplifts. These initiatives often require coordinated changes across the same participants, systems, specialist teams, and vendors. Poor sequencing can increase costs and operational risk, impair implementation quality, or divert capacity from higher-priority safety and modernisation work. Equally, waiting until the Review concludes in 2028 before progressing an urgent issue could allow existing material constraints to become entrenched or cause regulation to miss the investment decisions it needs to influence, especially once the implementation period of any new regulatory measures is taken into account. Issues for which delay presents those risks should therefore be progressed earlier, including independently of the broader Review timetable where appropriate. Lower-priority matters can remain under monitoring, including through the RBA's expanded information powers, and be sequenced behind relevant industry or regulatory processes until the evidence or need for intervention matures.

Merchant Choice & Competition

Merchant choice of payment methods and payment service providers (PSPs) can help strengthen competition, efficiency and safety in the payments system.[3] Consistent with the principles outlined above,

---

[3] In this submission, "payment service provider" (PSP) is used in a functional sense to refer to both banks and non-bank entities that provide payment services. Payment system operators and other technology providers are identified separately where their distinct functions are relevant.

competitive outcomes for merchants should be assessed across the breadth and quality of the propositions available, reflecting competition by providers across both price and the broader dimensions of efficiency such as functionality, service and safety, and the different value that merchants may rationally place on these features.

For merchant choice to exert competitive discipline, merchants need both credible alternatives and the practical ability to act on them, including through switching. Where merchants cannot readily act on an otherwise credible alternative, any regulatory assessment should consider whether this reflects legitimate differences among competing propositions, or a material constraint that merchants and otherwise viable competitors cannot reasonably overcome. The following subsections apply these considerations to specific aspects of merchant choice and competition identified in the Issues Paper.

Tokenisation and merchant credential portability

Tokenisation materially strengthens payments security, but its implementation should not prevent merchants from switching PSPs. The RBA should assess whether its May 2024 portability expectations are being met and, if material impediments remain, consider targeted measures formalising relevant elements of those expectations while building on the industry's existing technical arrangements.

AusPayNet supports the RBA's continued focus on tokenisation, which materially improves the security of online card payments by reducing reliance on primary account numbers (PANs). Effective credential portability is important to ensure that this security benefit does not come at the cost of merchants' practical ability to switch PSPs. Where a merchant's stored payment credentials cannot be migrated or securely replaced without undue friction, changing PSPs may require customers to re-enter their payment details or interrupt recurring payments. The resulting risk of customer attrition could make switching impractical, locking the merchant in with their existing provider. This is particularly relevant following the RBA's recent acquiring-transparency reforms, the effectiveness of which may be constrained if merchants are unable to act on the information provided. Since portability can depend on cooperation or processes outside the control of both the merchant and its prospective PSP, material constraints of this kind may warrant a targeted regulatory response.

In May 2024, the RBA established outcomes-based expectations that relevant industry participants support the portability of scheme and proprietary tokens so that merchants could change PSPs without undue friction.[4] AusPayNet coordinated the industry response, which recorded consensus that a lack of standardisation in information ported between gateways can cause merchant lock-in, and supported further industry work to address that constraint and improve portability. AusPayNet continues to support that position.

To support the industry in meeting the RBA's expectations, AusPayNet developed the *Standard for Payment Service Provider Porting of Merchant Payment-Related Data*.[5] The Standard establishes a common process for securely transferring merchant payment-related data between participating PSPs. However, because participation in the Standard is voluntary, it cannot ensure coverage across all relevant providers. This matters because effective portability depends on cooperation by both the sending and receiving PSPs, and the sending provider may have limited commercial incentive to facilitate a merchant's move to a competitor. The Standard therefore provides an important element of the

---

4 RBA (2024), *Expectations for Tokenisation of Payment Cards and Storage of PANs*, 23 May.

5 AusPayNet (2025), *Standard for Payment Service Provider Porting of Merchant Payment-Related Data*, June.

technical foundation for meeting the RBA's expectations, but cannot by itself ensure that the intended portability outcome is delivered across the market.

Indeed, the expectations have now been in place for more than two years, yet the Issues Paper notes that stakeholders continue to report difficulty migrating tokens between PSPs. AusPayNet therefore welcomes the RBA's reassessment of how effectively the May 2024 portability expectations are being met across the ecosystem. If the Review determines that material impediments remain and that existing measures are insufficient to meet the RBA's expectations, AusPayNet considers that formalising relevant elements of those expectations through targeted regulatory measures may be appropriate. Any such measures should establish the required portability outcome and appropriate coverage, with obligations directed to the participants or processes responsible for the remaining impediments. The measures should also build on the technical arrangements already established, allowing the AusPayNet Standard, scheme migration services, and other secure methods to provide the technical pathways for the relevant participants to meet them. This co-regulatory approach would preserve the progress achieved through industry coordination while providing enforceability where voluntary adoption cannot deliver the intended market-wide outcome.

Integrated platforms and bundling

Service integration and bundling can provide substantial benefits to merchants, and should not be treated as a systemic competition problem or subject to general unbundling requirements. Any material concern involving a particular platform or arrangement should be assessed by the appropriate regulators and addressed through a narrowly targeted response.

Integration and bundling are well-established forms of competition in the payments ecosystem. Banks, non-bank PSPs and technology platforms have long combined different payments services together, or bundled payments with broader business services. These arrangements may involve services designed to operate together, linked commercial terms, or both. A bank, for example, may provide acquiring alongside transaction accounts, lending and other services to business customers, with pricing and other terms that reflect the overall relationship. The ACCC recognises that tying and bundling are common commercial arrangements that usually do not harm competition, and can promote more compelling offers.[6]

As highlighted in the Issues Paper, recent years have seen notable growth in e-commerce and point-of-sale platforms that integrate payment acceptance into a broader suite of services supporting merchants' business operations. The Issues Paper recognises that merchants and consumers can benefit from the convenience of having such services integrated and supplied by one provider. However, the potential value of such 'convenience' for merchants should not be underestimated. Integrated platforms can reduce onboarding, implementation and coordination costs; seamlessly combine payment functionality with business software and other operational services; provide integrated support, security, fraud controls and service accountability; and offer predictable pricing and the recovery of joint costs across the complete proposition. The value that merchants may place on simplicity and reduced administrative burden was illustrated in the RBA's March 2026 MCPCS Review Conclusions Paper, which found that bundled pricing plans had become increasingly popular among small merchants despite generally charging higher fees, partly because they offer fee certainty and reduce the need to understand complex

---

[6] ACCC, *Misuse of market power—Tying and bundling*, accessed August 2026.

payment concepts. The growth of integrated platforms is similarly consistent with merchants valuing the wider operational benefits that such platforms can provide.

Competition involving integrated platforms can occur either between complete platforms and propositions, or within a platform where merchants can connect to competing PSPs. Effective competition does not require both forms to be available through every platform. Some providers may support external PSPs, while others may compete through a bundled proposition in which payments are a key element of the service design and commercial model. Legitimate reasons for retaining payments within a bundled proposition could include functionality, efficient cost recovery, security and risk management, service accountability, and continuing investment. A platform provider does not ordinarily have to redesign a differentiated product so that a rival can supply one revenue-generating component, while the merchant retains the benefits of the remainder of the platform on unchanged terms. A competing PSP's exclusion from one attractive platform, or inability to win those merchants through a lower standalone payment price, is not, by itself, evidence that competition is ineffective. Similarly, credential portability supports a merchant's practical ability to move, but does not create a right to retain every proprietary feature, discount or bundled benefit of the former proposition.

Genuine competition concerns could arise, however, where a broader platform becomes a commercially significant and difficult-to-bypass gateway, and its payment-related terms materially impede otherwise viable PSPs from competing for the merchants who depend on it. Any assessment of such concerns should consider whether merchants can move to a reasonably substitutable platform or assemble another service proposition without disproportionate disruption, and whether competing PSPs can reach the relevant merchant cohort through another practical channel. Where neither merchants nor competing PSPs can reasonably bypass the platform, payment-related restrictions or terms that exclude external PSPs – or make their use commercially impracticable – may materially impede otherwise viable PSPs from competing for the merchants who depend on it.

AusPayNet's current view of the broader ecosystem does not support treating integration and bundling as a systemic problem, or imposing general service unbundling requirements. Where stakeholder input to this Review identifies a potential competition concern involving a particular platform, provider or arrangement, the matter needs assessment by the appropriate regulator – either the ACCC or RBA depending on the entities and services involved. If a regulatory response is required, the preference is for an intervention that is narrowly targeted, and supports effective competition while preserving the benefits that integrated services can provide.

Account-to-Account Payments

AusPayNet supports the continued modernisation of A2A payments through the coordinated development of the A2A Payments Vision and Roadmap under the auspices of the A2A Roundtable, which includes the RBA. While some outcomes may require regulatory support, that need should be established through the Roadmap development process. The RBA should defer identifying specific regulatory priorities on A2A matters until the Roadmap is complete.

AusPayNet supports the continued modernisation of Australia's A2A payments system through an orderly, evidence-based and coordinated approach. As part of this, under ACCC authorisation, we helped establish and continue to facilitate the A2A Payments Roundtable, working alongside the RBA, Treasury and Australian Payments Plus (AP+) to shape the long-term direction of A2A payments. Through the development of the A2A Payments Vision and Roadmap, this work is intended to provide certainty to stakeholders and anchor investment in A2A products, services and underlying infrastructure over the coming years. In doing so, this joint process is addressing many of the substantive questions raised on this topic in the Issues Paper.

In July, the Roundtable published the A2A Payments Vision. The Vision sets out the outcomes that consumers, businesses and government agencies should be able to expect from A2A payments: a system that is safe, reliable, affordable, easy to use, and inclusive. It also identifies the system characteristics required to support these outcomes, including resilience, provider access, commercial viability, and appropriate standardisation. The Vision was informed by broad public consultation, workshops and bilateral engagement with end-users, banks, non-bank PSPs, technology companies, industry bodies, and government agencies. A summary of stakeholder submissions received through the consultation was published alongside the Vision, recording both agreement and divergence of views around challenges, ambition, priorities and trade-offs. AusPayNet considers that these documents provide a comprehensive and broadly tested articulation of current stakeholder views relevant to the future development of the A2A payments system.

The Roundtable is now focused on developing a practical pathway for delivering the Vision through the A2A Payments Roadmap. The Roadmap is expected to address many of the substantive A2A matters raised in the Issues Paper by establishing shared positions on: resilience, contingency and interoperability requirements; capabilities required for key payment use cases; security and consumer-protection requirements; areas where standardisation would be most beneficial; and access and participation frameworks.[7] Across these areas, the Roadmap will assess the available options and trade-offs, determine priorities and sequencing, identify key risks and dependencies, and clarify the roles and responsibilities of key stakeholders in delivering the A2A payments vision, including those of the public sector. The Roundtable has also established mechanisms for further input from end-users and other stakeholders to inform the development of the Roadmap.

AusPayNet expects that some outcomes necessary to realise the Vision may ultimately require regulatory support. However, the need for such support should first be established through the Roadmap process, which is still underway, and in which the RBA is actively participating. We therefore ask the RBA to defer reaching conclusions on any regulatory measures related to A2A payments as part of this Review until the Roadmap is complete. This will allow any future regulatory response to be informed by the Roadmap's evidence and outcomes, while avoiding a parallel process that could pre-empt or duplicate the Roundtable's work.

---

[7] Account-to-Account Payments Roundtable (2026), *The vision for account-to-account payments in Australia*, July.

Mobile Payments

Mobile wallets have delivered substantial competition and efficiency benefits, although longstanding uncertainty remains around effective access, issuer fees and contractual restrictions. Resolving whether current arrangements create material competition or efficiency concerns should be a priority outcome of this Review. The RBA and ACCC should coordinate a detailed assessment and, if material concerns are established, consider a targeted response that preserves security and investment incentives.

Over the past decade, mobile wallets have become an increasingly important part of Australia's payments ecosystem. The Issues Paper recognises the benefits they provide consumers, including convenience and strengthened security through tokenisation and biometric or device-based authentication. Mobile wallets have also supported other aspects of competition and efficiency in payments. For example, broad mobile wallets allow credentials from a range of institutions to be presented and accepted through a common interface. This enables issuers and acquirers of different sizes to support sophisticated and convenient payment functionality for consumers and merchants, without each having to develop and maintain a proprietary wallet. Mobile wallets have also enabled significant progress on merchant-choice routing of mobile debit transactions, and overseas developments indicate that similar interfaces may in time support retail A2A payments and competition across a wider range of payment rails at the point of sale.

However, the same aggregation that makes mobile wallets valuable could also strengthen the influence that a controller of a widely used device or wallet interface has over access, defaults, commercial terms, credential provisioning, and the distribution of competing payment methods. The Issues Paper identifies three distinct stakeholder concerns arising from this: access to device-level near field communication (NFC) functionality, fees and other costs borne by issuers, and contractual restrictions.

Concerns about access to NFC functionality have persisted for several years. The potential competition benefits of broader access have been recognised internationally, with regulators in several jurisdictions examining or acting on restrictions affecting third-party contactless services. Since the release of iOS 18.1 in October 2024, Apple has provided a published pathway for eligible third-party applications to access NFC and Secure Element functionality on iPhones in Australia, subject to eligibility requirements, technical permissions, product approval and a commercial agreement.[8] AusPayNet is not aware of any Australian provider that has publicly launched a competing contactless wallet on iPhone through this pathway. This may reflect legitimate commercial factors such as demand, product differentiation, customer reach, cross-platform scale, or sustainable economics. However, the confidentiality of access applications and commercial terms means that it is not possible to determine whether the Australian arrangements provide effective access, or whether pricing, functionality or other platform-controlled conditions are contributing to non-entry. The UK Competition and Markets Authority's (CMA's) recent preliminary view that Apple's access fees are likely to pose a significant barrier to entry in the UK strengthens the case for scrutiny of the equivalent Australian pathway.[9]

More specifically, we note that the Issues Paper focused on the concern that some mobile operating systems do not provide 'fee-free' direct access to NFC technology. However, AusPayNet does not consider that effective access necessarily requires a zero price. Providing secure access, certification, ongoing support and continued platform investment can involve real cost and value. Consistent with the

[8] Apple, *NFC & SE Platform for Secure Contactless Transactions*, accessed August 2026.
[9] CMA (2026), *Call for Evidence: Access to Near Field Communication functionality on Apple's mobile platform*, 30 June.

UK Competition and Markets Authority's high-level approach, any access framework should support contestability while allowing fair remuneration for efficiently provided services and preserving the platform provider's incentives to maintain and improve the underlying functionality. As part of this, per-transaction or ad valorem charges may merit particular examination where they scale materially beyond plausible cost or competitive value, or make a potentially lower-cost payment method uneconomic; however, they should also not be immediately presumed inefficient simply based on their structure.

Fees and other costs borne by issuers when transactions are initiated through an existing wallet raise a separate issue. The Issues Paper records stakeholder concerns about their current levels and possible future increases as mobile-wallet use grows. Such concerns may justify examination and proportionate monitoring, but do not of themselves support pre-emptive pricing regulation to guard against potential future changes. On the basis of current evidence, AusPayNet considers that confidential, ongoing regulatory visibility over relevant mobile-wallet fees and arrangements would be an appropriate near-term response. Public disclosure would serve a different purpose, and should not be treated as an automatic next step. Where issuers have limited ability to act on the information, publication may increase scrutiny without creating market discipline.

The same consideration applies to contractual restrictions on issuer disclosure of wallet fees – removing those restrictions may improve benchmarking or scrutiny, but would not necessarily create competitive discipline. If the RBA's assessment establishes material harm that confidential regulatory visibility alone will not correct, it could then consider appropriately aggregated reporting, fair-and-reasonable pricing principles, or other pricing governance directed to the identified problem. By contrast, contractual restrictions that prevent issuers from developing or supporting alternative payment methods, or steering customers towards them, could more directly constrain competition and innovation.

Given the growing importance of mobile wallets and the longstanding uncertainty surrounding effective access and related conduct in Australia, AusPayNet considers that reaching a substantive conclusion on whether current arrangements create material competition or efficiency concerns – and, if so, how these concerns should be addressed – should be a priority outcome of this Review. The three issues considered above may call for different responses, and effective and durable voluntary changes should be given a genuine opportunity to resolve any concern established. Because the issues involve both payment-system effects and wider platform-competition considerations, the RBA and ACCC should coordinate their assessment and any response. Any formal measure should be targeted to the identified problem and its source, while preserving security, consumer protection and incentives for continued investment.

Agentic Commerce

Agentic commerce should be treated as an important strategic monitoring and industry-engagement priority, but current evidence does not support agent-specific regulation. The RBA should monitor adoption and emerging standards, engage with relevant industry work and provide high-level policy orientation without introducing formal expectations at this stage.

Agentic commerce refers to a model of digital commerce in which AI-powered agents can act on behalf of consumers and businesses to initiate and complete transactions with some degree of autonomy. This extends beyond simply assisting customers with product discovery and recommendations ('AI-assisted shopping') – agentic commerce involves giving agents some level of delegated authority for payment-related decisions or actions, and can allow transactions to be initiated or completed without the customer's real-time involvement. This represents a significant shift from typical customer-initiated online transactions, such as card-not-present (CNP) payments, where the customer is directly involved at each step of the purchase initiation, checkout and authentication process.

The development of agentic commerce has accelerated significantly since 2025, although implementation and adoption remain at an early and controlled stage. Major payment networks, including Visa and Mastercard, have launched programs that enable AI agents to transact using tokenised payment credentials, building on existing network infrastructure and fraud controls. PSPs and technology companies have been developing toolkits, platforms and embedded checkout capabilities to support end-to-end agent-driven commerce. Controlled pilots, readiness programs, and early customer-facing implementations are now occurring across a growing number of markets. In Australia, Mastercard completed the first authenticated agentic transactions in January 2026, and Visa subsequently opened its Agentic Ready Program to Asia Pacific clients in April.[10]

The level of opportunity and risk presented by agentic commerce will depend on the authority and autonomy given to the agent. AI-assisted shopping can reduce search and comparison costs without taking any autonomous action on a customer's behalf. Greater delegation may provide additional convenience and improve customer outcomes by allowing agents to administer routine purchases, act at an appropriate time or price, and execute user preferences more consistently. For merchants, agentic services could create new channels for discovery and conversion, and reduce friction between product selection and payment. However, greater authority also increases the potential consequences of error, misuse or manipulation. An effective trust and liability architecture will therefore be critical to adoption at scale.

Trust and safety

In AusPayNet's view, the most critical and immediate policy questions around agentic commerce relate to trust and safety for consumers, merchants and payments system participants. In this context, agentic commerce raises three key challenges: establishing the identity of an agent, determining the scope of its delegated authority, and ensuring appropriate accountability and redress if something goes wrong:

- **Agent identity and authentication:** Payment participants and merchants need to be able to distinguish legitimate agents from malicious automated activity, and establish the consumer or business on whose behalf an agent is acting. This will require reliable and interoperable ways of identifying agents and signalling agent-initiated transactions across the payment chain.
- **Delegated authority and customer intent:** Merchants and payment participants also need reliable evidence that a legitimate agent is acting within the authority given by the customer. That authority may prescribe a specific transaction, or it may be qualitative or range-bound (for example, an instruction to make routine purchases, such as a weekly grocery shop, within a budget and according to a list of high-level preferences). The scope and limits of any delegated mandate therefore need to be capable of being expressed, evidenced, varied and revoked, with relevant information available to the participants in the transaction chain that need it for transaction acceptance, authorisation, risk assessment, and dispute resolution.

---

[10] Mastercard (2026), *Mastercard accelerates AI-powered commerce with Australia's first authenticated agentic transactions using Agent Pay*, 28 January; Visa (2026), *Visa Announces Global Expansion of Agentic Ready Program*, 29 April.

- **Accountability, disputes and redress:** Where a transaction is disputed, participants will need to establish whether the agent was legitimate, whether it acted within the customer's mandate, the nature of both any failure and liability regime. The appropriate treatment may differ depending on whether an agent or payment credential was compromised, the agent exceeded a valid mandate, or the customer disputes an agent's selection made within the mandate. Reliable evidence of the agent's identity and delegated authority will therefore be important to the effective operation of dispute, liability and consumer-protection frameworks.

The practical significance of these challenges will depend on the degree of autonomy involved. Current deployments commonly require explicit human confirmation of each transaction or operate within strictly predefined permissions. These constraints mean that current models can generally be accommodated more readily within existing payment, fraud and dispute processes than models involving broader delegated authority.

Importantly, the industry has strong incentives to address these core trust and safety challenges, recognising that agentic commerce is unlikely to scale otherwise. Consumers are unlikely to delegate their payment credentials and purchasing authority to services they do not trust, merchants will be reluctant to accept agents they cannot distinguish from malicious activity, and payment providers will not support transactions whose risks they cannot reliably assess and manage.

Consistent with these incentives, the development of agentic commerce capabilities has been accompanied by the rapid emergence of frameworks and protocols addressing the challenges discussed above. These are being developed by payment networks, technology providers and industry consortia around the world. Many are intended to be interoperable and payment-agnostic, but differ in their scope and technical approaches, meaning that some frameworks may be complementary in some respects and competing in others. The proliferation of different frameworks and the speed with which they are being developed and deployed may therefore create near-term challenges for payment providers, agent developers and merchants, including fragmentation and uncertainty about adoption pathways. In recognition of these risks, ore of this work is now moving into established standards bodies, including EMVCo and the FIDO Alliance, which may support greater coordination and convergence over time.

Competition and efficiency

Agentic commerce has the potential to affect competition and efficiency in both beneficial and adverse ways. The direction and significance of those effects will depend on the services, commercial models and adoption patterns that are still in the very early stages of forming.

For consumers, agents could reduce search and comparison costs, broaden their ability to discover competing merchants and products, and select more optimal payment methods according to their needs and preferences. For merchants, agentic services could create new channels for discovery and conversion. Verifiable evidence of customer intent could also provide merchants with stronger evidence when resolving disputed transactions, including cases of suspected first-party misuse fraud. Conversely, some models could allow an agent or platform to influence merchant visibility, payment-method selection, defaults, access or routing; steer transactions towards preferred providers; or introduce additional fees or access conditions. These effects are likely to vary across providers, service models, functions, and commercial arrangements.

Furthermore, as discussed earlier in relation to integrated platforms and bundling, integrating multiple functions or not supporting every competing provider is not, by itself, evidence that competition is ineffective. Early agentic products may legitimately support a limited range of merchants, credentials, payment methods or functions while safety controls and commercial models are tested; and these capabilities may expand as the technology and market develop. If a particular agentic service later becomes a commercially significant and difficult-to-bypass gateway, any potential concern would need to be assessed on the facts of that provider, function and arrangement, including whether consumers, merchants or competing providers have practical alternatives and whether any restrictions materially weaken competition without sufficient justification. This would distinguish genuine constraints on competition from legitimate product differentiation or limitations associated with an emerging service. At this time, however, we do not have evidence to support any material competition concerns involving a particular agentic service, or treating agentic commerce more broadly as presenting a systemic competition problem for the Australian payments ecosystem.

Recommended regulatory response

Given the early stage of market development, the substantial, controlled industry work underway to address safety and trust challenges, and the absence of an established material harm, AusPayNet recommends that the RBA treat agentic commerce as an important strategic monitoring and industry-engagement priority, rather than a priority for formal regulatory intervention at this stage. Current evidence does not support new agent-specific requirements concerning liability, access, routing, fees or neutrality. Prescriptive Australian requirements introduced before a domestic gap or material problem has been established could also duplicate or fragment global work, and constrain services and commercial models that are still developing.

Given the global and interconnected nature of payments, a significant proportion of the technical architecture and frameworks supporting agentic commerce will necessarily be developed internationally. The distinct Australian question is how emerging global standards, protocols and commercial arrangements interact with domestic payment systems, regulation, and industry frameworks. AusPayNet is currently developing an industry initiative to assess these questions, including how emerging global approaches to agent identity, delegated authority, and transaction evidence align with Australian payments frameworks, and whether any domestic gaps or coordination needs emerge. AusPayNet would welcome the opportunity to engage with the RBA as this work develops and relevant findings mature.

Over the coming years, the RBA should continue monitoring the movement from controlled deployments towards more autonomous or higher-volume use, developments in relevant international standards and their implementation in Australia, and whether material safety, competition or efficiency concerns emerge as the market develops. If the RBA has particular payments-policy outcomes it would like industry to keep in view, it should signal them at a high level through the conclusions to this Review. This should remain high-level policy orientation rather than a formal expectations instrument, technical checklist, intervention thresholds or pre-committed regulatory response. Such signalling would give industry useful direction, while preserving the flexibility needed as the evidence and market arrangements develop.

Cryptography & Security

Strengthening cryptographic protection across the payments ecosystem is a critical initiative that requires early and coordinated action. The RBA should support the prioritisation of this work through an enforceable standard establishing mandatory minimum outcomes for all critical payment systems, while allowing the industry to continue developing the technical implementation arrangements. This work should begin ahead of the Review's final conclusions, and be supported by coordinated readiness assessments for systems outside of the existing card migration program.

AusPayNet welcomes the RBA's recognition of the increasing importance of strengthening the cryptographic protections that underpin confidence in Australian payments. While the algorithms used across the payments ecosystem have served Australia well, advances in classical computing are reducing the protection offered by older standards. The anticipated emergence of cryptographically relevant quantum computers exacerbates this challenge, with the potential to render some of today's widely used encryption methods completely ineffective. The Australian Signals Directorate (ASD) has assessed that such capabilities could emerge as early as 2030 and become increasingly likely towards 2040.[11] Due to the interconnected nature of the payments industry, any system-wide cryptographic uplift will be highly complex and require long lead times. Early and coordinated action across the industry is therefore essential.

Card payments system

Recognising the need to respond to these evolving security threats, the industry has already made significant progress towards uplifting cryptographic standards for the card payments system. In late 2022, AusPayNet initiated the Advanced Encryption Standard (AES) Migration Program to coordinate the industry-wide transition from the Triple Data Encryption Standard (TDES) to AES. As highlighted in the Issues Paper, the operational complexity of this program is significant. The migration will affect almost every part of the card payment ecosystem, including schemes, issuers, acquirers, payment networks, terminals, ATMs, gateways and supporting technology providers. It will also require the replacement or upgrade of approximately 970,000 point-of-sale terminals and 25,000 ATMs.

Working closely with its members and other industry participants over the past four years, AusPayNet has developed the target state and Technical Blueprint, progressed with Standards Australia the necessary changes to the AS 2805 standard (which governs card-payment messages, cryptography and interoperability), established the migration and coexistence framework, and developed the industry testing strategy and supporting processes. The Program is now progressing to testing and pilot activity.

The AES Migration Program sets a staged implementation timetable that provides a coordinated path for different assets and functions across the card payments system to move towards the agreed cryptographic state. It begins with the AES sunrise date for new deployments on 31 December 2027, and proceeds to the general TDES sunset on 31 December 2030, with differentiated transport layer security and ATM milestones extending to 30 June 2032.

The migration to AES will materially strengthen symmetric protection in the card payments system. In parallel, AusPayNet has also commenced scoping a distinct industry workstream to address the risks that quantum computing presents to asymmetric cryptography. Asymmetric cryptography is used for a

---

[11] Australian Signals Directorate, *Planning for post-quantum cryptography*, accessed August 2026.

number of critical functions across payments, including authentication, digital signatures and key exchange. These functions currently commonly rely on traditional asymmetric algorithms such as Rivest–Shamir–Adleman (RSA) and elliptic-curve cryptography (ECC), which are considered vulnerable to quantum computing. Post-quantum cryptography (PQC) is designed to address these vulnerabilities. The ASD has recommended that Australian organisations develop their PQC transition plans by the end of 2026, begin the transition of critical systems and data by the end of 2028, and complete those transitions by the end of 2030. In line with this guidance, AusPayNet is working towards concluding the scoping exercise for the card-system asymmetric PQC migration by the end of the year.

While significant progress has been made on the AES Migration Program to date, AusPayNet is concerned about the industry's ability to meet the agreed milestones. In a recent survey, only 36 per cent of AusPayNet's issuer and acquirer members reported high confidence in meeting the required TDES sunset date in December 2030. Despite broad member support for the Program, participants are facing a number of significant implementation challenges. The primary challenge is delivering the migration in the context of many competing enterprise investment and change priorities. The migration must also be managed across a large installed base of payments hardware and supporting infrastructure, with different useful lives and replacement cycles. Some affected assets will not be due for replacement before the relevant Program milestones, requiring participants to bring forward upgrades or replacement that would otherwise have occurred through their normal technology refresh cycles. Program delivery will also depend on timely procurement, vendor readiness, and coordinated testing and implementation across many interconnected organisations.

Delayed implementation by some participants can have consequences for the wider card payments system. An uneven migration could prolong reliance on weaker cryptography and require counterparties to maintain legacy capabilities for longer, limiting the protection achieved across the card payments system. It could also expose individual participants to security and operational risks that they cannot fully address through their own actions. For example, the compromise of an acquirer that continues to rely on legacy cryptography could expose cardholder data associated with cards issued by other financial institutions. Those issuers may therefore remain exposed even after migrating their own systems. Timely migration across the entire ecosystem is therefore critical for delivering the intended outcomes of the Program.

Regulatory response

AusPayNet welcomes the Payments System Board's expressions of strong support for the industry's AES migration efforts to date, as well as its decision to consult on using the RBA's standard-setting powers to support this work.

Despite the significant progress made by parts of the payments ecosystem to proactively strengthen cryptographic standards, AusPayNet considers that the barriers to timely and comprehensive industry uplift warrant a co-regulatory approach. We therefore recommend that the RBA establish a strong, time-bound and enforceable cryptography standard for relevant payment systems. Under this model, the RBA would provide regulatory certainty and appropriate coverage by establishing and enforcing a mandatory minimum level of cryptographic protection across the systems in scope, drawing on standards developed by key domestic and international bodies. Industry participants would remain responsible for developing and implementing the technical arrangements required to achieve that outcome – including system architecture, testing and uplift pathways – and for maintaining compliance over time. For card payments, this co-regulatory approach would build directly on the technical and implementation foundations established through the AES Migration Program.

The standard should cover symmetric and asymmetric cryptography and include mandatory compliance timeframes for in-scope assets. AusPayNet has identified three elements that it considers should form the foundation of the standard:

- Strong cryptography, including quantum-resistant cryptography where relevant, should protect payments in transit and payment data at rest. The protection of payments in transit includes the need for confidentiality, integrity and authorisation.
- Cryptographic algorithms should provide protection equivalent to AES-128 or higher and be standardised, specified or otherwise recognised by relevant international standards bodies, including the International Organization for Standardization (ISO), the Internet Engineering Task Force (IETF), and the US's National Institute of Standards and Technology (NIST).
- Cryptographic keys should be protected and managed across their full lifecycle in accordance with established standards such as NIST SP 800-57 and ISO 11568.

These principles would establish the regulatory floor while allowing the supporting technical standards and implementation arrangements to evolve with technology, threats and international standards. For each payment system within scope, compliance timeframes should be mandatory and reflect system- and asset-specific implementation pathways. For the AES Migration Program, the established industry milestones should provide the foundation for those timeframes. This would preserve a mandatory common outcome while allowing the implementation sequence to reflect the condition and dependencies of each system. AusPayNet welcomes the opportunity to continue working with the RBA on the detailed design and system-specific application of the standard.

It is important to note that the value of the standard for the cards-focused AES Migration Program will depend on when regulatory certainty is provided. Major investment, procurement, asset-replacement and testing decisions are already being made by industry participants to ensure readiness by December 2030. To ensure that regulatory certainty arrives while it can still alter the critical implementation path, we encourage the RBA to consider prioritising the development of the proposed cryptography standard ahead of the final conclusions of the broader Review in 2028.

Other critical payment systems

The need to maintain contemporary cryptographic protection extends across all critical payment systems in Australia. Each system, whether publicly or privately operated, therefore needs to assess its current cryptographic settings against this requirement and identify any uplift needed. Where uplift is required, a coordinated program of work will need to be established across the system operator, its participants, relevant service providers and shared infrastructure. AusPayNet has already commenced an analysis of whether cryptographic changes are required for the Bulk Electronic Clearing System (BECS) and the High Value Clearing System (HVCS) and will share the results of this analysis with the RBA in due course.

To support prioritisation of this work across the payments ecosystem, AusPayNet considers that the standard proposed above should apply to all critical payment systems. The RBA should also consider coordinating structured assessments of cryptographic readiness across systems, working with the responsible operators and participants. These assessments should establish each system's current cryptographic state and any existing uplift initiatives, identify material dependencies and risks, and determine the scope and sequencing of the work required. The results should inform practical system- and asset-specific pathways and compliance timeframes under the proposed standard, supporting a consistent minimum level of protection through implementation arrangements that reflect each system's architecture, exposure, asset life, readiness and technical requirements. Together, these measures would provide a durable foundation for maintaining effective cryptographic protection across the Australian payments ecosystem as technologies and threats continue to evolve.

Overseas Card Payments Fraud

While overseas card fraud is an important safety and efficiency issue, the ongoing scheme, issuer, and coordinated industry work is the most appropriate near-term response. The RBA should allow this work to progress before considering formal action, with AusPayNet keeping it informed as the evidence base and industry response mature.

The proliferation of scams and fraud in Australia poses a significant threat to our society, economy, and digital ecosystem. As part of our strategic priorities, AusPayNet is committed to working with members, government, regulators, and other stakeholders to help defend the payments system and its users against economic crime. We therefore welcome the RBA's consideration of overseas CNP fraud as a regulatory priority. As highlighted in the Issues Paper, overseas CNP transactions represented only around three per cent of spending on Australian-issued cards in 2024, but accounted for around half of the fraud recorded on them. This is a significant concentration of fraud within a relatively small pool of transactions, which rightly raises concerns about its possible impact on system safety and efficiency.

It should be acknowledged that the true impact of overseas CNP fraud on the Australian payments system and consumers is difficult to quantify. The $454 million gross fraud value reported in the published 2024 statistics is likely to differ substantially from the cost ultimately borne in Australia. The RBA's Issuer Cost Study provides a useful indicative starting point. For Australian-issued CNP transactions acquired outside Australia, the study reports net issuer fraud and fraud-prevention costs of 24 basis points of transaction value, with a further 3 basis points for disputes, chargebacks and write-offs.[12] The combined 27 basis points cost is around one-quarter of the published gross overseas CNP fraud rate of around 121 basis points. Applied to the value of overseas CNP transactions in 2024, this suggests Australian issuer costs of around $100 million. The difference between gross fraud and issuer costs is consistent with the expectation that a substantial share of fraudulent transaction value would be allocated to overseas acquirers and merchants through chargebacks. Interchange fees received from overseas acquirers may further offset some of the remaining issuer costs. Nevertheless, even where a significant portion of transaction losses are recovered, Australian issuers continue to bear the costs of prevention, investigation, customer service, dispute handling and card replacement. Similarly, even when consumers are refunded for any fraudulent transactions, they may still bear costs such as the loss of access to their card or funds, legitimate transactions being declined, and broader inconvenience and time loss. Persistently high fraud could also affect confidence in card payments over time. Overseas CNP fraud therefore remains an important issue for the Australian payments ecosystem, even if the actual cost is materially lower than the gross fraud value.

---

[12] RBA (2025), *Review of Merchant Card Payment Costs and Surcharging: Issuer Cost Study*, 19 August.

Fraud prevention tools

Recognising the potential impact of fraud on consumer trust and safety, and the disproportionate share of CNP fraud relative to the total, the Australian payments industry has introduced a range of measures to strengthen fraud prevention over recent years. The combination of these measures has seen domestic CNP fraud rates decline materially. An important part of this response was AusPayNet's implementation of the CNP Fraud Mitigation Framework in 2019 through the Issuers and Acquirers Code Set. Where fraud thresholds are breached, the Framework can require remediation or impose sanctions, including a requirement to implement Strong Customer Authentication (SCA). This provides a valuable common mechanism through which industry participants and merchants can be held to agreed standards, strengthening the shared incentives to respond to elevated fraud risks.

The Issues Paper considers whether applying SCA requirements to overseas CNP transactions could extend some of these benefits to the overseas fraud channel. In card e-commerce, SCA is generally requires the *merchant* or its payment service provider to initiate an authentication exchange with the issuer. This exchange gives the issuer additional transaction and device information and, where necessary, enables it to challenge the cardholder before the transaction proceeds. However, overseas merchants and acquirers sit outside of both AusPayNet's Framework and the RBA's regulatory remit, and an Australian SCA rule directed at issuers cannot require them to initiate or participate in this process. Where an overseas merchant does not support SCA, an issuer can still seek confirmation from the cardholder before deciding whether to authorise the transaction. While this may look similar to a merchant-initiated authentication exchange from the perspective of the cardholder and issuer, the merchant has not initiated the exchange or received a recognised authentication result, the issuer may have less transaction context, and the ordinary liability treatment may not apply. A universal issuer SCA requirement would therefore be more likely to operate as an effective decline or decline-and-retry rule in many cases, potentially leading to the rejection of many legitimate transactions and increasing customer friction without improving merchant-side adoption. It could also cause particular disruption for large online retailers that process substantial absolute fraud amounts simply because of their transaction volumes, even where their fraud rates are comparatively low. AusPayNet therefore does not support a blanket SCA mandate on domestic issuers, as the instrument is mismatched to the cross-border architecture and could impose disproportionate costs. If stronger authentication is pursued, it should be risk-based and applied where it can reduce fraud without imposing disproportionate costs on legitimate transactions.

Beyond a blanket SCA mandate, Australian issuers and the international card schemes retain a range of tools that can help address the problem. As the Issues Paper notes, some issuers have already adopted additional step-up authentication processes for certain overseas CNP transactions without a formal requirement. Issuers can also apply separate risk-based confirmation or decline controls at authorisation, although these have different coverage, data, customer-experience and liability characteristics from merchant-initiated authentication exchanges. Other technologies, including payment tokenisation, remote checkout solutions such as Secure Remote Commerce, and device-based cardholder verification through digital wallets, can also reduce the exposure of card credentials or provide stronger customer and device signals. International card schemes also apply measures such as merchant and acquirer monitoring, remediation programs, credential intelligence, and network risk controls to address overseas fraud. These measures are complementary: issuers can strengthen how they respond to transactions presented to Australian card accounts, while the schemes can influence the broader global environment in which overseas merchants and acquirers submit those transactions.

Industry and regulatory response

Recognising the value of industry coordination for addressing economic crime, AusPayNet is currently developing a program of work with its members on card fraud and scam mitigation. This program will include a dedicated workstream on overseas CNP fraud, which is expected to examine practical industry measures to address the issue, including issuer-side controls and global engagement through the international card schemes. Potential areas for consideration and assessment under this workstream may include authentication coverage, the distribution of fraud losses and prevention costs, the extent to which available data distinguish unauthorised transactions from first-party misuse, and the effects of different measures on fraud, transaction approvals and customer experience. This work should provide a stronger shared evidence base for identifying the most effective industry response, and assessing whether any residual problem may later warrant regulatory attention.

With the industry proactively engaged in addressing overseas CNP fraud, and given the limitations of an isolated issuer-side SCA mandate, AusPayNet does not consider that regulatory intervention on this issue is warranted at this stage. We recommend that the RBA allow current issuer, scheme and coordinated industry work to progress before considering any formal action. AusPayNet would nevertheless welcome the opportunity to keep the RBA informed as this work develops. If the program identifies a significant issue that the industry cannot adequately address, we would also welcome the opportunity to work with the RBA on the design of any regulatory response, to ensure that it would address the demonstrated problem in a targeted, effective and proportionate way.

Conclusion

AusPayNet welcomes the RBA's Review as an important opportunity to ensure that Australia's payments system regulation remains fit for purpose as the ecosystem continues to evolve. As set out in this submission, regulatory priorities should be guided by clear evidence of material public interest concerns, with responses targeted and proportionate to the problem identified, and building on effective industry arrangements where possible.

AusPayNet looks forward to continuing to engage with the RBA as it determines its regulatory priorities and progresses the next stages of the Review. We would welcome the opportunity to work with the RBA to support a regulatory framework that promotes competition, efficiency and financial safety while maintaining the payments system's capacity to deliver secure, reliable and innovative payment services.

Yours sincerely,

Andy White
Chief Executive Officer
Australian Payments Network