Response to Reserve Bank of Australia, Review of Payments System Regulation

Issues Paper June 2026

17 August 2026

Introduction

Mastercard welcomes the opportunity to respond to the Reserve Bank of Australia's (**RBA**) Review of Payments System Regulation - Issues Paper (**the Review**). Retail payment systems are key infrastructure for a productive digital economy. They affect how efficiently consumers, merchants, financial institutions and digital platforms transact, manage risk, reconcile activity and adopt new technology. The Review is therefore relevant not only to competition, efficiency and financial safety in the payments system, but also to Australia's broader productivity, innovation and economic growth agenda as AI, agentic commerce, tokenisation, real-time account-to-account payments (A2A), digital wallets, cryptographic uplift and increasingly sophisticated fraud reshape commerce.

While productivity is not an express statutory objective of the Payments System Board (PSB), it is directly relevant to the RBA's mandates to promote efficiency, competition and financial safety, and to direct payments policy to the greatest net-benefit of merchants, consumers and the broader economy. A payments system that reduces friction, supports trusted digital commerce, enables automation and strengthens resilience promotes efficiency in practical economic terms. Conversely, regulation that focuses narrowly on short-run acceptance costs, or slows investment in secure and interoperable next-generation payment capability, may weaken productivity, competition and innovation outcomes over time.

This is consistent with the Government's broader focus on productivity, regulatory reform, innovation and AI-enabled growth agenda. The productivity challenge Australia faces is longstanding: the Treasurer has noted that productivity growth over the last full decade was the slowest in 60 years[1]. By contrast, EY-Parthenon modelling estimates that AI could add AUD$95 billion to AUD$116 billion to Australia's economy by 2036, supported by a 2.0 to 2.4 per cent uplift in multifactor productivity[2]. Future policy or regulatory decisions should therefore be risk-based and outcomes-focused, so responsible AI-enabled and agentic payment models can deliver their full benefits for merchants, consumers and the broader economy by reducing friction, automating workflows, strengthening fraud prevention and improving choice.

AI-enabled commerce, tokenisation, A2A, digital wallets, cryptographic uplift, digital assets and rising fraud are reshaping how consumers, merchants and financial institutions transact. The RBA's approach should avoid a narrow cost-only lens and instead support a secure, competitive and resilient multi-rail ecosystem that encourages investment, and promote full realisation of economic and productivity benefits from next-generation retail payments.

Mastercard supports the Review as an issue-identification and prioritisation stage in a broader reform process, rather than a vehicle for immediate prescriptive intervention across all topics.

[1] Turning headwinds into tailwinds – Australia's productivity challenge
[2] The economic upside of Artificial Intelligence for Australia | EY - Australia

Mastercard's submission is framed around three principles:

1. The PSB's objectives should be assessed through a system-wide value and productivity lens, including economic contribution, security, resilience, innovation and consumer protection, rather than cost metrics alone.

2. Competitive neutrality and a level playing field should be prioritised by assessing like activities by economic substance rather than formal category, so regulation applies consistently where payment arrangements perform comparable functions.

3. Regulation should remain proportionate, risk-based, outcomes-based and technology-neutral, particularly for A2A payments, agentic payments and cryptographic uplift, so innovation and adoption can proceed, while safety and trust are maintained.

This value lens of retail card payments is central to Mastercard's submission. Retail card payments provide significant net value to merchants and the Australian economy through faster checkout, lower cash-handling costs, higher conversion, better reconciliation, fraud protection, chargeback rights, security, resilience and consumer confidence. Efficiency should therefore not be assessed solely by reference to merchant fees or acceptance costs. Deloitte Access Economics estimates that card payments contributed AUD$38.7 billion to the Australian economy in 2022, equivalent to 1.8 per cent of GDP, and saved around 46 million labour hours across hospitality, leisure and retail trade[3].

Next-generation capabilities will amplify that value. AI, tokenisation, agentic commerce and advanced fraud and security tools can automate payment and reconciliation workflows, strengthen fraud prevention and support safer, more resilient commerce. Mastercard Safety Net has helped stop more than US$77 billion in fraud globally over the last decade[4], underscoring why the value of security and fraud prevention should be considered alongside cost. If regulation views these developments mainly through fees and costs, Australia risks constraining investment and missing a generational opportunity to capture the productivity and economic benefits of next-generation payments. Mastercard therefore encourages the RBA to apply its competition, efficiency and financial safety mandate through a system-wide assessment of value alongside cost.

To support the RBA's objectives of competition, efficiency and financial safety, Mastercard makes the following policy recommendations:

1. **Weigh productivity and value alongside cost**: Ensure the PSB's competition, efficiency and safety mandates assess payments system value, including productivity, economic contribution, security and innovation, not cost alone.

2. **Refresh the PSB Statement of Expectations**: The Treasurer should update the PSB's Statement of Expectations, unchanged since 2018, and invite a new Statement of Intent that reflects the Government's broader growth,

[3] The value of Australia's retail payments system | Deloitte Australia
[4] Beyond one billion: inside the journey to a more inclusive and sustainable economy | Mastercard Global

productivity, competition, regulatory reform and innovation priorities, including the role of trusted digital infrastructure and AI-enabled commerce in lifting productivity.

3. **Designate three-party networks that meet a functional-equivalence test**: Assess three-party networks by economic substance and designate those that perform the same economic function as four-party networks. At a minimum, the RBA should formally assess whether there are equivalent shadow interchange or comparable merchant fee disclosure issues.

4. **Keep A2A regulation outcome-based and technology-neutral**: Support designation of the NPP under the PSRA as a proportionate perimeter step, while focusing any standards or access requirements on outcomes, including access, interoperability, consumer protection, ecosystem fraud controls and resilience, rather than prescribed infrastructure or governance models.

5. **Support responsible AI-enabled payments innovation:** Any RBA expectations for agentic and AI-enabled payments should be principles-based, risk-based and aligned with international standards, supporting productivity, merchant and consumer choice, competition, efficiency, financial safety and trust.

6. **Align cryptographic uplift with international standards**: Anchor expectations in international standards bodies and multilateral coordination mechanisms rather than Australia-specific requirements.

7. **Support market-led merchant choice in digital payments**: Encourage competition, transparency and configurable merchant choice across mobile, online and agentic payment environments, with routing and selection decisions based on cost, capability, security, functionality and value rather than mandatory lowest-cost rules.

Opportunity and Risk of Agentic Commerce

Agentic commerce should be treated as a distinct productivity, competition and risk issue for the Australian economy. If deployed safely, agentic payment capabilities can help translate AI's broader productivity potential into practical retail-payment outcomes by helping merchants and consumers automate discovery, checkout, authentication, invoicing, recurring payments and reconciliation. Poorly governed models could create risks around consent, identity, fraud, liability, transaction visibility and fragmented proprietary protocols.

External analysis underscores the scale of this shift. McKinsey estimates that agentic commerce could orchestrate up to US$1 trillion in US B2C retail revenue by 2030, with global projections reaching US$3 trillion to US$5 trillion[5]. This reinforces why agentic commerce should be treated as a primary policy area in this Review.

[5] Agentic commerce: How agents are ushering in a new era | McKinsey

Australia is well placed to support trusted agentic commerce, given its advanced payments infrastructure, high digital adoption and strong history of payments innovation.

RBA policy settings will be fundamental to whether that opportunity is realised in retail payments. The RBA should support open competition within common international standards and security boundaries, enabling trusted and interoperable agentic payment solutions while allowing providers to compete on capability, user experience, fraud prevention and speed to market. The focus should be on ensuring merchants can make informed choices between competing payment options, and that providers are free to compete on value, security, functionality and cost as agentic payment models develop. Verified agentic-payment frameworks can also provide safer and more transparent participation than unmanaged agent activity, supported by agent verification, tokenised credentials, consent capture and transaction visibility.

Merchant choice in payments

Mastercard supports merchant choice, consumer choice, transparency and competition between payment options. The policy objective should be to ensure that merchants can make informed, configurable and value-based choices across mobile, online and emerging agentic payment environments. That choice should reflect cost, capability, security, functionality, consumer expectations and overall value, rather than treating lowest-cost routing as the primary policy objective. Providers should be able to compete to deliver better outcomes for merchants and consumers through value, security, functionality, reliability and cost.

Where a payment is routed or presented in a way that changes the applicable protections, consumers and merchants should have clear information about the payment rail used and the protections that apply. This is particularly important in mobile, online and emerging agentic payment environments, where routing and selection can be affected by issuer, acquirer, wallet, gateway, PSP and merchant configuration settings.

The RBA's findings indicate that competition is already operating in debit payments, including through the availability of alternative network capability. Enabling LCR can lower debit acceptance costs, and net scheme fees for online debit acquiring fell across all networks after eftpos introduced online functionality in 2022/23.

The key policy point is that competitive constraint can arise from credible capability and informed merchant choice, not only from routed volume. Regulation should therefore promote transparency, merchant configurability and pass-through, while allowing providers to compete on capability, security, functionality and value.

The current expectations-based approach has also delivered progress, with in-person LCR enablement increasing from 50 per cent of merchants in June 2022 to 84 per cent by December 2025.

Importantly, the RBA has also recognised that some merchants, or acquirers acting on their behalf, choose not to enable LCR for non-price, value-based reasons.

The same principles should apply in online and mobile environments. Availability of routing capability is important, but effective choice also depends on gateway, PSP, tokenisation, wallet and merchant configuration settings. The RBA's focus should be on whether merchants and consumers have the information and practical ability to choose between payment options, and whether providers can compete on cost, security, functionality, fraud protection, reliability and innovation.

Mastercard supports tokenisation and secure portability that enables merchants to switch payment service providers or gateways without unnecessary friction. The priority should be completing the shift away from stored unencrypted Primary Account Numbers (PANs) and ensuring tokenisation is secure, reliable and widely adopted. Portability should support secure merchant switching and credential migration where feasible, not require tokens to be detached from the trust, security and lifecycle controls that make tokenisation effective.

Mastercard supports portability and migration models that preserve issuer validation, token lifecycle controls, fraud controls and transaction context. We do not support proprietary or network-bound tokens being used outside the security framework for which they were created, or proprietary gateway or PSP tokens being treated as interchangeable network tokens. Network tokens are created within a chain of trust between the issuer, cardholder, merchant and network, and are bound to a specific environment, such as a merchant app or website, so compromised token data cannot be reused elsewhere. Where migration is needed, it should occur through secure re-tokenisation or standards-aligned processes that preserve issuer control, cardholder data protection and ecosystem trust.

Mobile payments, non-designated card networks and BNPL

Mobile wallets raise important competition and transparency considerations. Mastercard supports a fair and level playing field in which all providers can compete to offer secure, convenient and innovative payment experiences, subject to appropriate security and consumer-protection standards.

Mobile wallets and wallet-enabled payment methods can increase consumer convenience, security and competition. Regulatory settings should support fair and transparent access to payment functionality, while preserving high standards for device security, tokenisation, authentication, fraud prevention and consumer protection. Where wallet-enabled A2A functionality develops as an alternative to cards at the point of sale, comparable expectations should apply so consumers and merchants understand the protections, liability arrangements and dispute processes associated with each payment option.

Three-party networks and competitive neutrality

Competitive neutrality should guide the RBA's assessment of three-party networks, non-designated networks and BNPL where those arrangements perform comparable payment system functions. Three practical principles should guide that assessment:

1. Regulation should be function-based where the relevant activity can be identified and assessed by economic substance, including wholesale fee flows, equivalent shadow interchange, merchant acceptance economics and arrangements that perform the same economic function as regulated interchange.

2. Where formal regulation is not yet justified or the perimeter remains uncertain, equivalent transparency and reporting should apply so merchants, consumers and regulators can compare the true cost and competitive effects of competing payment arrangements.

3. Where formal regulation is not currently applied, regulatory settings should preserve market discipline rather than entrench asymmetry by extending advantages such as surcharge prohibition to higher-cost unregulated schemes without equivalent transparency, reporting or regulatory obligations.

These principles are relevant to three-party networks and other non-designated payment arrangements where merchant-facing fees, cardholder incentives, acceptance rules or acquiring-partner models may have similar competitive effects to regulated payment arrangements. The RBA should assess these arrangements by economic substance rather than formal category and consider whether equivalent transparency, reporting or regulatory expectations are warranted.

The public-interest concern is therefore broader than equal treatment between schemes. Functionally equivalent payment activity should face equivalent rules, equivalent transparency or effective market discipline. This framework is expanded in Q8.

Similar issues may arise for other non-designated networks, alternative acceptance arrangements and BNPL providers where they perform comparable payment-system functions for merchant acceptance. The relevant policy question is whether equivalent activities are subject to equivalent transparency, consumer protection, fraud prevention and regulatory expectations.

Account-to-account payments

Mastercard supports the development of A2A payments and operates real-time payment systems in other markets. We have actively and constructively engaged with AusPayNet and Australian Payments Plus (AP+) on the A2A roundtable and draft A2A Vision for Australia. A2A should be free to compete with cards on its merits, provided it offers consumers comparable expectations for security, authentication, consumer protection and fraud protection.

Domestic debit arrangements should also be assessed through a competitive-neutrality lens. Existing DNDC issuance and routing settings, and combination credit card arrangements, should be periodically reviewed to ensure they continue to support competition on the merits and remain justified by clear public-interest benefits in today's digital, tokenised and mobile payment environment. The objective should not be to inadvertently disadvantage any particular domestic or

international network through regulatory settings, but to ensure that regulatory settings remain fit for purpose as payment technology, fraud controls, digital wallets and A2A rails evolve.

Ensuring A2A and domestic debit compete on their merits

As noted above, domestic debit networks are relevant to online and mobile routing, consumer protections and merchant configurability. In the A2A context, the broader issue is competitive neutrality: whether historical domestic debit settings should be carried forward into emerging rails or digital environments without a current public-interest assessment. The Issues Paper helpfully distinguishes competition between cards and A2A from development within A2A, but that framing would be strengthened by more explicit consideration of how existing domestic debit settings interact with future A2A, NPP, tokenisation and DNDC policy choices.

Domestic debit capability is relevant to online and mobile routing, consumer protections and merchant configurability. Broad availability should be distinguished from demonstrated consumer or merchant preference in particular digital payment use cases. The RBA should consider whether existing settings continue to promote competition on merit, as digital capability, tokenisation, fraud controls and consumer experience become increasingly important to competitive value.

Cryptography and fraud prevention

Mastercard supports the RBA playing a facilitative and coordinating role in industry-wide cryptographic uplift, particularly where coordination can help align participants, clarify expectations and support timely implementation across the payments ecosystem. However, that role should avoid duplicating, displacing or cutting across existing domestic and international standards, regulatory frameworks and industry-led initiatives, including the AES Migration Program and PCI guidance.

Cryptographic uplift should proceed through clear phases, reflecting the scale and complexity of an ecosystem with a large and diverse set of participants, devices and service providers. A staged approach would allow industry to prioritise higher-risk use cases while ensuring that upgrades remain internationally interoperable and aligned with global standards. Mastercard's post-quantum readiness program, including our Quantum Security and Communications program and partnership with IBM on quantum-resistant payment solutions, sits alongside emerging coordination through the G7 Cyber Expert Group and Europol's Quantum Safe Financial Forum. Timelines for quantum or broader cryptographic uplift should align with the AES Migration Program and international post-quantum standards, recognising that the risk is not only future-dated: ASD has warned that encrypted data captured today may be vulnerable to "harvest now, decrypt later" attacks, and the G7 has noted that quantum capabilities able to defeat current cryptography could emerge within a decade[6].

[6] https://www.cyber.gov.au/business-government/secure-design/quantum/planning-for-post-quantum-cryptography

External modelling of a quantum-enabled attack on a major real-time gross settlement system estimates direct losses of US$730 billion to US$1.95 trillion, equivalent to 3.2 to 8.6 per cent of US GDP, and indirect losses of US$2 trillion to US$3.3 trillion[7].

Cryptographic uplift should also be considered alongside authentication technology. As payments move further into digital wallets, passkeys, device-bound credentials and biometric authentication, safety will depend on stronger encryption and secure, user-friendly ways to verify identity, consent and transaction intent. Regulation should support phishing-resistant authentication and biometric capabilities where they reduce fraud, while ensuring liability frameworks and the ePayments Code keep pace.

Mastercard supports continued efforts to reduce overseas card-not-present (CNP) fraud on Australian-issued cards, which is now overwhelmingly concentrated in online, digital transactions, particularly at overseas merchants. As outlined in the Issues paper, RBA data shows card fraud on Australian-issued cards reached AUD$913 million in 2024, with CNP fraud accounting for around 90 per cent of that value and overseas merchants contributing disproportionately. However, any response should be proportionate, risk-based and aligned with global standards. A blanket requirement for issuers to apply SCA to all overseas CNP transactions may increase customer friction and false declines without addressing the offshore merchant and acquirer-side drivers of fraud. Mastercard would support targeted, intelligence-led measures that strengthen fraud prevention while preserving security, efficiency and cross-border interoperability. Please refer to our response in Q18.

Other issues to consider

The Review should also be considered in the context of several significant payments reform workstreams already underway, including Treasury's payments licensing reforms, the A2A Payments Roundtable, the AES cryptographic-uplift program, the Scams Prevention Framework, digital identity, and broader work on digital money, tokenised assets and the National AI Plan. These workstreams are interconnected and should be sequenced and aligned so regulatory decisions are coherent, avoid duplication and support industry's capacity to invest and innovate.

This alignment is important to ensure payments regulation complements the Government's broader economic priorities, including productivity growth, innovation, competition and risk-based regulatory reform. The RBA's approach should focus on clear outcomes, consistency across related reforms and proportionate implementation, so payments regulation supports competition, efficiency and financial safety while enabling trusted innovation in retail payments.

[7] Prosperity at Risk: The Quantum Computer Threat to the US Financial System | Hudson Institute

Question responses

Merchant choice in payments

Q1. What are the impediments to competition between debit card networks for merchants' transactions on DNDCs across mobile and/or online environments? Are there practices by industry participants that limit competition, efficiency or financial safety in relation to debit card transactions?

Competition between debit card networks on DNDCs in mobile and online environments is affected by two known issues today. First, issuing and provisioning settings can determine whether international and domestic debit credentials are available and capable of being routed in mobile wallets, tokenised environments and stored-credential use cases. Where the practical availability of a network depends on issuer, wallet or token-provisioning configuration, merchant choice may be constrained even where LCR is technically available.

Second, commercial deal frameworks between schemes, acquirers, PSPs, gateways and integrated platforms can shape routing outcomes. These arrangements may bundle routing with broader acquiring, gateway or platform services, or create incentives that influence how merchants or providers configure routing. The relevant policy issue is transparency and merchant control: whether merchants can understand the commercial, technical and service implications of routing choices and configure those choices based on cost, capability, trust and value, rather than having routing outcomes determined by opaque bundled arrangements or automatic lowest-cost settings.

Mobile, online and agentic payment environments are developing quickly. Regulation should encourage participants to build within common international standards for tokenisation, authentication and fraud prevention, while competing on capability, security, trust, user experience and value. Merchant choice should therefore be informed, configurable and value-based, with consumers having visibility of the payment rail used and the protections that apply. This approach supports competition and innovation without reducing routing or payment selection to least cost alone.

Q2. Is there a public interest case for the RBA to take further action to support competition across debit card networks in mobile and/or online environments?

There is a public interest case for supporting competition across debit card networks in mobile and online environments. That case should be directed to informed, configurable and value-based merchant choice, supported by consumer choice, visibility and protection. The RBA should support merchant configurability, transparency, pass-through monitoring and consumer visibility, while allowing networks and service providers to compete within common international standards on capability, security, trust, user experience and value. These settings will also be important as agentic payment models develop, because merchants will need the ability to choose payment solutions based on the value they deliver, not only headline cost.

Mastercard supports the RBA's policy objectives and supports a principles-based framework that allows those objectives to be met through secure, scalable and globally consistent architecture. As payment technology evolves, including tokenisation, Click to Pay, numberless cards, passkeys, digital wallets and agentic commerce, merchant routing choice should be enabled through outcome-based principles that preserve flexibility, security and innovation while allowing networks to compete through their own technical solutions.

Further RBA action should focus on outcome-based expectations, transparency and monitoring rather than prescriptive transaction-level routing rules. A principles-based approach focused on informed merchant configurability, consumer visibility, transparency, pass-through monitoring and consumer protection is more proportionate and better supports competition based on value, security, functionality and cost.

That distinction is material to the public interest test. The RBA describes LCR as operating through two channels:

1. a direct reduction in costs on transactions actually routed, and

2. an increase in competitive pressure on debit networks to lower their wholesale fees[8].

The public interest test should therefore focus on practical outcomes: whether merchants can access and configure competing payment options, whether consumers understand the rail and protections that apply, and whether providers can compete on capability, security, reliability and value. Where those conditions are met, competition can operate through market-led choice without prescriptive routing mandates.

Q3. How difficult is it for merchants to switch away from their existing integrated platform services provider to access their preferred PSP? To what extent do merchants receive clear and sufficient information from integrated platform providers prior to joining about potential challenges in switching PSPs, and are there areas where greater transparency could help them better understand potential costs and risks?

Integrated platforms that combine payments with e-commerce, point of sale, invoicing, inventory or customer-management services can create material switching frictions for merchants. The issue is not only whether merchants can compare PSP prices, but whether they can retain their preferred PSP, switch PSPs without degrading payment functionality, and understand the practical consequences before onboarding. Switching may require merchants to reconfigure integrations, migrate stored credentials, update recurring-payment arrangements, rebuild tokenised customer profiles, change checkout or invoicing workflows, and manage customer communication where payment credentials need to be re-established.

[8] https://www.rba.gov.au/payments-and-infrastructure/review-of-retail-payments-regulation/2026-03/conclusions-paper/pdf/conclusions-paper.pdf

Greater transparency should therefore focus on switching consequences, token and credential portability, and continuity of payment functionality, not only headline payment fees.

Integrated platform providers should clearly disclose before onboarding whether payment credentials, tokens, recurring-payment mandates, customer profiles, reporting data and reconciliation workflows can be transferred, re-tokenised or otherwise migrated to another PSP, and what steps, costs, timeframes and customer impacts are involved. While network tokens must remain subject to issuer, scheme and security controls, merchants should be able to understand whether PSP or gateway proprietary tokens can be migrated without unreasonable cost, delay, customer disruption or loss of core payment functionality. The RBA should encourage competition within integrated platforms by supporting merchant transparency, PSP choice and secure migration between PSPs where feasible.

Q4. Does the bundling of payments with other services, such as in integrated platforms, raise competition, efficiency and/or financial safety issues in the payments system? If so, should regulatory action be considered and what form should it take?

Bundling payments with other services through integrated platforms can generate both benefits and risks. On the positive side, bundled offerings can improve efficiency and user experience: merchants receive integrated reporting, unified support, streamlined onboarding and tighter linkage between payments, inventory and accounting. On the risk side, bundling can create lock-in where merchants are effectively required to use a particular PSP or acquiring arrangement to access non-payment services they value, which can weaken competition in the underlying payments market.

From a competition and efficiency perspective, the key question is whether bundling arrangements materially impede merchant choice over payment providers or obscure the true cost of embedded payment services.

From a safety perspective, bundling can also concentrate operational and security risk if the integrated platform does not maintain appropriate standards. Regulatory action, if considered, should be targeted and outcome-based: focused on transparency and ability for merchants to switch to alternative PSPs rather than prescribing business models. Ensuring merchants receive clear information about payment costs and contractual terms within bundled arrangements, and can move payments to alternative providers without disproportionate barriers, would preserve the benefits of integrated platforms while mitigating the risks of lock-in.

Q5. How do stakeholders assess the functioning and effectiveness to date of the RBA's tokenisation expectations? Is further regulatory intervention needed to promote the portability of tokens for payment cards, or to address other competition, efficiency or financial safety issues associated with implementing tokenisation across card payment systems? If so, what regulatory actions should be considered?

The RBA's tokenisation expectations, finalised in December 2023 and updated in May 2024, have reinforced the industry's shift away from storing raw funding PANs and toward broader adoption of network tokenisation. Mastercard supports that direction and considers the priority should be accelerating the secure rollout of tokenisation, while allowing current portability work to mature and ensuring competitive neutrality where one network relies on infrastructure funded and operated by another.

Tokenisation is becoming core to enabling seamless and secure payments infrastructure and will increasingly co-exist with passkeys, biometric authentication, device-bound credentials and other security layers. It will also be foundational to agentic payment use cases, where agents should not handle raw PANs or reusable credentials and where tokenised credentials, authentication and transaction context will be central to maintaining trust. Regulatory expectations should therefore align with international standards and support secure, interoperable adoption across the ecosystem.

ASIC's planned major update to the ePayments Code should keep pace with these developments and be sequenced coherently with the new Scams Prevention Framework. Tokenisation, digital wallets, passkeys and biometric authentication are increasingly part of the same payment credential and authentication environment, but uncertainty in liability settings can limit the rollout of stronger authentication technologies. In particular, clearer treatment is needed where a consumer authenticates using biometrics, a device-bound credential or a passkey but later disputes the transaction because of fraud, scam activity or misuse. Industry needs certainty on how the ePayments Code and Scams Prevention Framework (SPF) will interact so participants can invest confidently and adopt stronger authentication at pace. The RBA should work with ASIC and Treasury to refresh the Code more frequently so liability outcomes support, rather than inhibit, adoption of phishing-resistant authentication, biometric verification and other technologies that improve security, trust and consumer experience.

On portability, further regulatory intervention should be cautious and standards-aligned. The RBA's end-June 2025 deadline for same-network token portability has passed, while cross-network synchronisation was deliberately given a longer runway. AusPayNet's *Industry Position on the RBA's Tokenisation Expectations*, published in April 2024, identified genuine technical constraints, including immature token synchronicity and limited quality metrics on active and inactive tokens. While wider adoption of the PAR may in the future support interoperability, PAR was designed as a scheme-specific identifier and is not currently shared with third parties due to security considerations. Any future PAR-based model will require careful consideration of security implications for cardholders, as well as intellectual property and personal data implications. The RBA should also distinguish token portability from secure migration between PSPs or gateways. Mastercard supports merchant switching where feasible, but any migration model must preserve issuer validation, token lifecycle controls, fraud controls and the transaction context needed for authorisation, monitoring and dispute handling.

Network tokens are issued, validated and lifecycle-managed within a trust framework that involves issuers, cardholders, merchants and payment networks.

Any token migration or portability model should preserve issuer validation, token lifecycle controls, fraud controls, transaction context and dispute-handling integrity. Mastercard supports merchant switching where feasible, but migration models should not compromise cardholder data security or ecosystem trust.

The RBA should also consider competitive neutrality in tokenisation-related use cases. Where participants rely on shared infrastructure or common services, the allocation of cost, risk and benefit should remain transparent, proportionate and consistent with secure adoption of tokenisation across the ecosystem.

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?

Agentic commerce is part of a broader shift as consumers, merchants and small businesses adopt AI-enabled tools for product discovery, comparison, purchasing and business workflows. The RBA's focus should be on the point at which those tools operate as agents in the payment flow, including where they initiate, facilitate or execute a transaction on behalf of a consumer or business. Relevant payment-system outcomes include agent identification, credential security, authenticated consent, verifiable transaction intent, transaction visibility, fraud controls and liability allocation.

These tools create productivity opportunities where they automate business workflows, improve customer journeys and reduce operational friction. For merchants and small businesses, agentic commerce may deliver benefits beyond payment execution through workflow automation, inventory management, cash-flow and expense management, reconciliation and improved customer experience.

The relevant payment-system issues arise most clearly when those tools operate as an agent by initiating, facilitating or executing a payment on behalf of a consumer or business. At that point, the key questions are:

1. Is the agent identifiable?

2. Has the consumer authorised the agent to act within a defined transaction scope?

3. Are credentials secured through tokenisation so that agents do not handle PANs or reusable card credentials?

4. Are ecosystem participants able to receive the transaction context needed to assess legitimacy and manage fraud risk?

5. Is there reliable evidence for dispute handling and liability allocation?

Any response to agentic payments should be directed to the RBA's payment system objectives of competition, efficiency and financial safety, while supporting productivity, risk-based innovation and trust. Payments-specific expectations should focus on the outcomes needed for safe agentic commerce and remain aligned with the Australian Government's broader approach to AI governance.

Mastercard's Agent Pay capability, built on existing tokenisation and authentication frameworks aligned to international standards such as EMVCo and FIDO passkeys, and the Verifiable Intent standard co-developed with Google, illustrates how verified agentic payment models can build safely on existing payment rails and security frameworks. Key safeguards include identifiable and verified agents, cardholder authentication, verifiable consumer consent, tokenised credentials, transaction intent, ecosystem visibility and reliable dispute evidence. Agent identification and registration should be risk-based, proportionate and non-discriminatory, so smaller agents, merchant agents and new entrants are not excluded where they can meet equivalent trust and security requirements. The immediate regulatory priority should be outcome-based safeguards for consent, identity, transparency, interoperability, dispute handling and liability allocation, rather than pre-emptive restrictions on agentic payment models or endorsement of any particular product architecture. Purpose-built agent-specific liability rules should be considered only if existing frameworks prove insufficient.

A further policy issue for the RBA is interoperability, because interoperable standards are central to security, risk management and trust in agentic commerce. If agentic commerce develops through fragmented or proprietary protocols for merchant discovery, cart formation, consent capture and payment execution, merchants may face higher integration costs and potential lock-in to particular agents, PSPs, acquirers, or networks. The RBA should therefore support the development of common, open and internationally aligned agent–merchant–payment standards that enable trusted participation without creating a closed access layer, while allowing different providers to compete on security, reliability, user experience and value. This approach is consistent with Mastercard's support for open and internationally aligned standards and does not require the RBA to endorse any particular agentic payment product or architecture.

Following the Prime Minister's 15 July 2026 announcement on Australian Standards for AI, RBA expectations for agentic payments should align with the emerging national AI governance framework and internationally aligned standards. The RBA's role should be to address payment-system outcomes such as authentication, transaction visibility, dispute evidence, interoperability and financial safety, while broader AI-specific issues are addressed through the national framework.

Agentic AI should also be assessed through the RBA's financial safety and payments critical infrastructure regulatory role. Properly governed agentic AI can support payment-system resilience by improving threat detection, alert triage, vulnerability prioritisation, incident response and fraud-pattern identification.

The Australian Cyber Security Centre (ACSC) recognises these cyber-defence opportunities while warning that agentic AI services require careful adoption, including governance, human oversight, least-privilege access, defined operating boundaries, monitoring, testing and auditability[9]. The RBA should therefore ensure that any expectations for agentic payments preserve the responsible use of agentic

[9] https://www.cyber.gov.au/business-government/secure-design/artificial-intelligence/careful-adoption-of-agentic-ai-services

AI, rather than creating payments-specific requirements that could slow secure deployment.

Mobile payments, non-designated card networks and BNPL

Q7. Are there competition, efficiency and/or financial safety issues relating to mobile payments? If so, are there any regulatory actions that the RBA should consider?

Mobile payments raise competition, efficiency and safety issues that warrant careful consideration, particularly where wallet architecture, access to payment functionality, device-level rules or wallet-provider arrangements affect competition, routing capability, security responsibilities or liability outcomes. Mastercard supports competition in mobile payments, including fair and transparent access to payment functionality, provided regulation preserves high standards for security, tokenisation, authentication, fraud prevention and consumer protection and does not impede innovation in fast-developing wallet and device environments.

Any regulatory response should remain outcome-based and competitively neutral. Wallet and device providers should support fair and transparent access to payment functionality while meeting equivalent standards for security, tokenisation, authentication, identity controls, fraud prevention and consumer protection. Liability frameworks should be clear and should reflect the role each participant plays in the payment chain. This approach would address key risks without unduly constraining innovation or prescribing particular technical models.

This assessment should include not only device-based wallets but also major digital wallet and acceptance providers where they facilitate merchant acceptance, consumer payment initiation, payment presentation or routing in mobile and online environments. Where such providers perform material payment-chain functions, equivalent transparency and reporting should apply so regulators can assess their impact on competition, efficiency, financial safety, security and consumer outcomes.

Q8. Are there competition, efficiency and/or financial safety issues relating to three-party networks? If so, what regulatory action should the RBA consider?

Yes. Mastercard considers there may be competition, efficiency and transparency issues where three-party networks or related acceptance models perform functions comparable to regulated payment arrangements. The relevant question is not whether a provider fits neatly within a particular business model category, but whether the economic substance of the activity has similar effects for merchants, consumers and the broader payments system. Where merchant-facing fees, acceptance rules, cardholder incentives or acquiring-partner arrangements create comparable competitive effects, equivalent transparency, reporting or regulatory expectations should be considered.

The functional-equivalence case should be assessed by reference to economic substance and effect, not contractual form. This includes whether the arrangement performs functions analogous to regulated wholesale or acquiring arrangements, whether fees or incentives influence acceptance economics, and whether merchants

and regulators have sufficient transparency to compare competing payment options on a like-for-like basis. International approaches that examine functional equivalence provide useful context for this assessment.

The case for RBA action should be framed around practical responses. First, the RBA should require equivalent transparency and reporting where non-designated networks or acquiring-partner models perform material payment functions. Second, regulation should apply where functional equivalence can be identified and where the activity raises material competition, efficiency or financial safety issues. Third, where formal regulation is not applied, market discipline should remain effective through transparency and comparable disclosure so merchants and consumers can assess competing payment options.

This approach is consistent with Australia's national competition policy architecture, which favours broad, economy-wide application of competition principles and treats departures from competitive neutrality as requiring clear, transparent and public-interest justification. Amex's current regulatory treatment appears to reflect historical categorisation rather than a contemporary assessment of functional equivalence, competitive effect and public benefit.

If the RBA is not prepared to proceed to designation following this Review, intermediate steps would still advance competition, efficiency, transparency and perimeter integrity. These could include enhanced reporting of merchant fee data, clearer disclosure of arrangements that materially affect acceptance economics, and ongoing monitoring of whether current regulatory treatment remains justified by public-interest considerations.

Q9. Does the current regulatory treatment of non-designated card networks such as JCB and UnionPay remain appropriate given their limited scale in Australia, or would formal regulation of these networks by the RBA better support competition, efficiency and financial safety in the payments system?

JCB and UnionPay present narrower but distinct competitive-neutrality issues. Where UnionPay operates as a four-party network, the relevant question is whether equivalent regulatory treatment should apply where it performs the same economic function as designated four-party card schemes, particularly if volumes, merchant fee levels or cross-border pricing become material. Where JCB operates through three-party or acquiring-link arrangements, including its acquiring relationship with Amex in Australia, the RBA should apply the functional-equivalence framework set out in Q8.

Q10. Are there competition, efficiency and/or financial safety issues relating to BNPL services? If so, what regulatory action should the RBA consider?

BNPL services raise competition, efficiency and financial safety issues along three dimensions: costs and surcharging, market structure and transparency, and fraud, identity and scam-related risk as BNPL becomes increasingly embedded in mobile and online commerce. On cost, the RBA's data shows BNPL merchant fees have declined materially, from around 4.5 per cent in 2020 to around 3.0 per cent in 2025, but remain several times higher than the four-party card networks, and no-

surcharge rules mean these costs continue to be embedded in retail prices and cross-subsidised by consumers who do not use BNPL. On market structure, increasing concentration in the BNPL sector, including the withdrawal of smaller providers from some segments, works against the competitive discipline that would otherwise be expected to continue narrowing this fee gap over time. On transparency, BNPL providers typically do not publish merchant fees, limiting merchants' ability to benchmark costs or negotiate effectively, which we consider a straightforward efficiency gap the RBA could address through disclosure requirements without touching BNPL's underlying commercial model.

BNPL can also create financial safety risks where onboarding, account management and fund flows are not supported by strong digital identity and fraud controls; synthetic identities, account takeover, mule activity, first-party fraud and deepfakes used to bypass remote onboarding and authentication are increasingly relevant. A proportionate regulatory response should therefore avoid treating BNPL purely as a pricing or surcharging issue. The RBA could consider outcome-based, technology-neutral expectations requiring BNPL providers to be transparent about costs and key rules, including publication of merchant fees, while also demonstrating appropriate identity, fraud and dispute controls throughout the customer lifecycle.

The RBA should not need to classify BNPL as either a three-party or four-party card scheme to bring it within an appropriate regulatory perimeter. The better approach is functional: where BNPL services perform a comparable payment-system function and raise competition, efficiency or financial safety issues, the RBA should consider designating BNPL as a payment system under the PSRA. Designation would ensure BNPL is treated as a designated system capable of being made subject to applicable RBA standards, rather than remaining outside the core payments regulatory perimeter. It would also support similar surcharging treatment across comparable payment systems, helping to avoid distortions where higher-cost BNPL acceptance is treated differently from designated card systems.

This is also relevant to Treasury's broader incoming payments licensing framework because of recent amendments effective from 19 December 2025 to the Corporations Regulations 2001 to exclude facilities that are payment systems designated under the PSRA from being treated as a financial product and therefore Australian financial services licensing requirements. Designation would therefore support clearer and more coherent regulatory treatment of BNPL for payments-system standards, including surcharging, as well as Australian financial services licence considerations as part of Treasury's payments licensing reforms.

Account-to-account payments

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?

Australia's A2A ecosystem is at an important decision point as participants consider the future of bulk and batch processing alongside the continued growth of instant payment use cases. Key challenges relate to access, decentralised clearing and participation models, interoperability, fraud prevention and long-term certainty.

These challenges can limit efficiency, competition and financial safety across the payments system.

Access to BECS and NPP infrastructure remains complex and costly, particularly for fintechs, non-bank providers and new entrants. Participation often involves multiple clearing and settlement relationships, bilateral arrangements and scheme-specific rules, increasing implementation cost and time to market. Australia's decentralised clearing model also requires participants to manage multiple technical integrations and standards, making it harder to create uniform end-user experiences.

Consumer protection and fraud prevention arrangements for A2A payments are also more fragmented than in card schemes. Cards operate within mature scheme frameworks that define fraud controls, chargeback and dispute processes, liability rules and recovery mechanisms for a wide range of "unhappy paths". A2A protections, by contrast, can differ between institutions, and there is no single ecosystem-level rulebook, a gap that limits consumer trust and adoption, particularly in real-time environments where speed and irrevocability increase exposure to social-engineering scams.

Finally, many critical payment services continue to rely on BECS capabilities, including bulk payroll, direct debits and bill payments.[10] Participants need greater certainty about how these capabilities will be preserved, modernised and connected to instant payment infrastructure as the ecosystem evolves; without a clear roadmap, essential bulk services risk remaining on legacy platforms longer than optimal and investment risks becoming reactive rather than coordinated.

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?

There is a case for targeted RBA action on A2A payments, focused on access, architecture, consumer protection and ecosystem fraud controls. Any action should remain outcome-based and technology-neutral, and should be delivered through the transparent governance and roundtable processes already underway, consistent with the RBA's Public Interest Framework for a Successful A2A payments system.

The current decentralised clearing model can increase cost, slow innovation and limit contestability, particularly for smaller and newer participants. The RBA's role should be to set outcome-based objectives for access, interoperability, resilience and comparable clearing and settlement capability across A2A schemes, rather than prescribe a single infrastructure or governance model. Preserving scope for multiple providers, including international schemes and domestic infrastructure, would allow the market to determine the most efficient architecture and support competition in bulk payments, BECS replacement pathways and future real-time or near-real-time A2A services.

Comparable access to clearing and settlement capability will be important to competition. Where common settlement infrastructure, including RITS or fast settlement services, is available to one scheme or infrastructure provider, access

[10]RBA, Review of Payments System Regulation – Issues Paper, June 2026

arrangements should be transparent, risk-based and available on equivalent terms to other appropriately regulated schemes that can meet operational, security and financial safety requirements. This would support resilience and redundancy, reduce single-rail dependency and allow competition to occur on service quality, functionality, reliability and value rather than infrastructure access.

From a resilience perspective, regulatory action should support a future-state architecture in which instant and bulk services operate as complementary components of a multi-rail ecosystem, consistent with the RBA's own observation that greater use of payment methods on different rails can help maintain confidence and control risk to the financial system if one system experiences disruption. Decisions on governance, competition mechanisms or infrastructure design should follow completion of the roadmap and roundtable consultation process, and should maintain an outcome-based and technology-neutral approach rather than mandating specific technical solutions.

Regulatory support is also warranted where it promotes consumer trust and ecosystem reliability. Fraud and scams cut across institutional and geographical boundaries; without common rules, reporting and liability allocation, responses remain fragmented. The RBA could support common standards for fraud reporting, dispute management and liability apportionment; ecosystem-level fraud data; network-level detection; and a streamlined dispute platform operating under pre-agreed rules.

With respect to the NPP, it is no longer an emerging payment system. Its growing role in A2A payments raises public-interest issues relating to access, participation complexity, consumer protection, real-time fraud and scam exposure, resilience, standardisation, interoperability and migration from legacy A2A infrastructure.

Mastercard recommends that the RBA designate the NPP as a payment system under the Payment Systems (Regulation) Act 1998. Designation would not require immediate prescriptive intervention, but would ensure that the RBA has an appropriate regulatory perimeter for a system that is now systemically important to A2A payments and raises public-interest issues relating to access, interoperability, consumer protection, fraud and scam controls, resilience, migration from legacy A2A infrastructure, and equivalent transparency and reporting where A2A schemes perform comparable payment-system functions.

This approach is consistent with a level-playing-field principle: payment systems that perform material account-to-account functions should be subject to appropriate oversight, without prescribing a particular technology, governance model or commercial architecture.

Q13. What are the barriers to more seamlessly enabling A2A payments in the in-person and online environments through, for example, digital wallets, and do they warrant the RBA taking action to address them?

Several barriers currently limit the more seamless enablement of A2A payments in in-person and online environments, including through digital wallets. The fragmented access and participation model across A2A infrastructures can slow the

adoption of overlay services such as Pay by Account and A2A at point of sale, because consistent connectivity and rules across institutions are required to deliver these services at scale.

Many digital wallets are primarily designed around card rails, and integrating A2A options in a way that offers comparable user experience, security and merchant integration requires common standards for identity, authentication, payment initiation and routing. Where such standards are immature or implemented inconsistently, A2A options may remain niche within wallets and online checkouts. Trust gaps versus cards are also relevant: differences in speed, irrevocability, dispute rights and protections can make users reluctant to choose A2A options for higher value or business-related transactions.

These barriers suggest that regulatory action should focus on enabling conditions rather than mandating specific solutions. The RBA could support industry work on common A2A standards for wallet integration, and encourage transparent disclosure of the rail used and its characteristics, speed, irrevocability, dispute processes, protections and price, so consumers and businesses can make informed choices at the point of payment. Maintaining an outcome-based, technology-neutral approach will allow A2A and card providers to innovate on experience and functionality while meeting common expectations for safety, transparency and competition.

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

Regulatory action can play a constructive role in promoting standardisation and interoperability across cards and A2A payments, particularly through messaging standards, settlement flexibility and transparency. As a first priority, the industry should work towards adoption of ISO 20022 across all A2A payment infrastructures, including both instant and bulk payment use cases. A common messaging standard would simplify integration, improve interoperability between payment systems and facilitate innovation in reconciliation, risk controls and value-added services.

As part of a longer-term payments vision, the RBA may also encourage convergence between card and A2A ecosystems through the gradual migration of card processing infrastructure from legacy ISO 8583 messaging towards ISO 20022-based models where practical. Standardisation efforts should extend beyond messaging to encompass settlement: it remains important to preserve support for deferred net settlement within RITS, including bulk settlement of card and A2A payment positions, alongside continued real-time settlement capability.

The RBA should also encourage common services that can be utilised across schemes where this improves efficiency, resilience and trust, including fraud and scam detection, identity and authentication, dispute handling, reporting, tokenisation, agent–merchant–payment interoperability and other value-added services. These services should be developed in a way that preserves competition between schemes and providers, avoids unnecessary duplication, and enables participants to adopt shared capabilities without locking the market into a single provider or governance model.

Finally, as cards and A2A rails become more closely integrated in wallets and online checkouts, regulatory focus should include transparency and informed choice. End users should have clear, accessible information on which rail is being used and its relevant characteristics, speed, irrevocability, dispute handling, protections and price. This transparency would allow consumers and businesses to make payment decisions based on the criteria most important to them, and would support genuine competition across rails rather than competition obscured by inconsistent presentation.

Cryptography and fraud prevention

Q15. How is the payments industry strengthening its cryptographic practices in response to evolving cyber threats? What initiatives or uplift programs are underway, whether led by individual participants, industry bodies, or international standard-setting groups, and how effective are these initiatives likely to be in delivering an appropriate and sustainable level of cyber security?

The payments industry is strengthening cryptographic practices through a combination of internal uplift programs, coordinated industry initiatives such as the AES Migration Program[11], and alignment with international standard-setting bodies. Mastercard's approach is deliberate, phased and risk-based: conducting comprehensive cryptographic inventories to identify and prioritise at-risk systems; assessing the quantum and cryptographic readiness of critical suppliers; transitioning key systems to NIST-approved algorithms where appropriate; and maintaining ongoing monitoring of the threat environment. Our Quantum Security and Communications program and our partnership with IBM on quantum-resistant payment solutions sit within this broader effort.

We support a risk-based sequencing of cryptographic uplift that prioritises the protections most relevant to today's transaction environment. In the near term, that means completing tokenisation, expanding the use of dynamic cryptograms and short-lived keys, and strengthening cryptographic agility across the ecosystem. These controls materially reduce the value of compromised credentials and give single-use transaction tokens a different risk profile from long-lived sensitive data. Quantum risk remains important and requires preparedness, but immediate regulatory and industry effort should focus on practical uplift aligned with ISO, EMVCo and AP+ work on AES migration. We support the AP+ AES program, while recognising that delivery depends on issuers, acquirers and other ecosystem participants. This uplift should also sit alongside device-bound credentials, biometrics and passkeys, so cryptography, authentication and transaction intent operate as part of a consistent security experience.

AES-128 remains widely accepted for many use cases when properly implemented. Mastercard is therefore focused on maintaining current security while advancing cryptographic agility and post-quantum readiness. Industry efforts should remain anchored in international standards, including NIST, ISO, EMVCo, IETF, PCI DSS and guidance from relevant cybersecurity agencies. New multilateral coordination

[11]AusPayNet, 'Advanced Encryption Standard (AES) Migration', May 2026.

through the G7 Cyber Expert Group and Europol's Quantum Safe Financial Forum reinforces the case for global alignment rather than jurisdiction-specific mandates.

Q16. What key barriers or challenges are participants facing in uplifting cryptography and broader cyber security practices within the payments system?

Uplifting cryptography across the payments system is inherently complex, reflecting the scale and heterogeneity of the ecosystem. Key barriers include long-lived infrastructure with limited cryptographic agility, the AES Migration Program alone involves an estimated 970,000 point-of-sale terminals and 25,000 ATMs requiring replacement or upgrade, dependencies on third-party providers and standards, incomplete visibility of cryptographic assets, and differences in resources and capabilities across institutions, with smaller institutions that are nonetheless critical to systemic resilience often facing the greatest constraints.

A further practical challenge is sequencing uplift across participants at different stages of readiness. Some ecosystem participants are still completing baseline tokenisation, AES migration and cryptographic-agility work, while larger institutions are already planning for post-quantum readiness. This uneven maturity means the RBA should avoid treating cryptographic uplift as a uniform compliance exercise. A more effective approach would prioritise short-lived keys, dynamic cryptograms, tokenisation and AES migration as near-term baseline protections, while supporting longer-term post-quantum planning through internationally aligned standards and realistic implementation timelines.

Post-quantum cryptography illustrates a further, more fundamental barrier: differing guidance between industry-preferred incremental, hybrid migration approaches and broader national security guidance favouring a faster, more comprehensive uplift, compounded by genuine uncertainty about both the timing of the quantum threat and the best sequencing of the response. These barriers suggest cryptographic uplift should be viewed as an ongoing, coordinated transformation rather than a single event, dependent on clear and interoperable standards, realistic timelines that recognise infrastructure lifecycles, support for smaller institutions, and mechanisms to share threat intelligence and best practice across the ecosystem.

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 can play a valuable role by promoting alignment with interoperable, globally recognised standards, convening industry dialogue, encouraging preparedness for post-quantum cryptography, and maintaining an outcome-based, technology-neutral regulatory stance. Harmonised security expectations are essential for organisations operating across multiple jurisdictions; the RBA can reinforce the importance of adopting standards from bodies such as NIST, ISO, EMVCo and the PCI Security Standards Council, and avoid mandating Australia-specific cryptographic requirements that might fragment global interoperability or increase implementation burden disproportionately.

In the context of post-quantum cryptography, the RBA could support sector-wide preparedness by promoting awareness of emerging risks, facilitating industry coordination and information sharing, and reinforcing alignment with internationally recognised standards and guidance. Regulatory expectations should remain focused on resilience, interoperability and cryptographic agility, while allowing institutions to determine the most appropriate implementation approach based on their individual circumstances and technology roadmaps.

The RBA is best placed to facilitate structured dialogue among payment schemes, financial institutions, technology providers and regulators, including roundtables focused on cryptographic uplift, threat intelligence and migration planning, and to encourage institutions to plan and build cryptographic agility while emphasising alignment with established standards bodies such as EMVCo. Rather than specifying particular algorithms or implementation approaches, the RBA's expectations could focus on outcomes: maintaining strong cryptographic protection, ensuring the ability to migrate when standards change, and managing systemic risk, while respecting differences in infrastructure and risk profiles across institutions.

See also the fourth recommendation in our response to Q19, which proposes a targeted regulatory safe harbour for RBA-convened payments coordination activities. Such a safe harbour would be particularly relevant to cryptographic uplift, because it would allow the RBA to convene and supervise industry-wide migration planning, threat-intelligence sharing and implementation coordination without each public-interest coordination process requiring a separate ACCC authorisation.

Q18. Do current arrangements for addressing overseas card not present fraud raise competition, efficiency and/or financial safety issues? Should the RBA consider a regulatory response to these issues, and if so, what form should this response take?

The domestic CNP Framework, enforced through AusPayNet's Issuers and Acquirers Community Code Set, has worked in reducing CNP fraud at Australian merchants. But it does not reach overseas merchants and acquirers. The result is a safety, efficiency and competition issue: fraud costs are absorbed by issuers and ultimately reflected in payment-service pricing, while dispute and chargeback burdens fall on consumers and issuers.

Current arrangements rely on network-level rules and technologies and global industry-standard framework specifications, including EMV 3-D Secure (EMV 3DS) for cardholder authentication in e-commerce transactions, issuer and acquirer fraud monitoring, and scheme dispute processes. International experience under PSD2 shows that strong customer authentication can reduce CNP fraud while preserving user experience when combined with risk-based decisioning.

Biometric authentication and passkey-based verification should be central to this evolution, but adoption will be accelerated only if the ePayments Code provides clearer liability treatment and the Scams Prevention Framework is finalised in a way that gives industry certainty for transactions authenticated through biometrics, device-bound credentials or passkeys and later disputed because of fraud, scam activity or misuse.

Building on Mastercard's acquisition of Recorded Future, Mastercard Threat Intelligence has been launched specifically for payment fraud. In its first three quarters, Threat Intelligence identified more than 7 million card-testing transactions across 192 countries. Stopping that activity prevented an estimated US$172 million in fraud linked to malicious domains, delivering real value for Mastercard, its customers and cardholders.

Mastercard supports stronger controls for overseas CNP fraud but prefers risk-based authentication. A blanket mandatory SCA requirement for all overseas CNP transactions could add friction, increase abandonment and false declines, and may not address the root cause given the RBA's jurisdictional limits over overseas merchants and acquirers. Measures imposed only on Australian issuers and acquirers are unlikely to address fraud driven by overseas merchant and acquirer environments, compromised credentials, weak authentication practices and cross-border data and enforcement limits.

Continued investment in risk-based authentication tools implemented through EMV 3DS and associated issuer/acquirer fraud controls and monitoring, reinforced by risk-based authentication expectations aligned with international standards and improved fraud data sharing, is more proportionate than a blanket mandate.

Other issues

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?

There are several cross-cutting issues that the RBA should consider prioritising to promote competition, efficiency and financial safety in the payments system.

First, scams, including authorised push payment fraud, have become a global epidemic, with significant financial and trust impacts. Experience from other markets shows that coordinated, ecosystem-level approaches can materially reduce these losses. In the UK, multi-bank, network-level scam detection models analyse a high proportion of A2A transactions in real time, using multi-institution data to assess risk on both the sending and receiving accounts. Participating banks have reported significant improvements in scam detection and reductions in reported fraud volumes after deploying such models. These outcomes underline that individual institutions cannot fully address scams on their own: effective detection requires multi-bank, ecosystem-wide views of transaction patterns. The RBA could support common scam reporting and reimbursement rules, shared intelligence and risk-scoring capabilities, and privacy-aware data-sharing frameworks for scam prevention. This should be coordinated with the recently enacted SPF and ASIC's refresh of the ePayments Code, so industry has clearer and more consistent expectations on scam prevention, liability, reimbursement and data sharing.

Second, competitive neutrality and reform sequencing are important cross-cutting themes. As this submission explains, asymmetric regulation of functionally similar activities, whether between cards and A2A, domestic and international schemes, or designated and non-designated networks, can distort competition and investment incentives. The RBA's regulation should continue moving toward function-based assessments grounded in economic substance, risk and public-interest justification rather than historical categories.

Third, the Treasurer should refresh the Statement of Expectations for the PSB, last updated in 2018, to clarify how the PSB should monitor and manage existing and emerging risks while ensuring regulatory interventions remain proportionate and do not focus solely on cost reduction. Given the Government's recent Statements of Expectations for APRA and ASIC, which reflect its broader agenda on economic growth, competition, innovation, technology, AI and productivity through proportionate, risk-based regulation, payments regulation should be aligned.

Fourth, Treasury should consider a targeted regulatory safe harbour for RBA-convened payments coordination activities where the RBA determines that coordination is necessary or desirable to promote competition, efficiency, resilience, access or financial safety in the payments system. The recent cash-distribution experience illustrates the problem: banks, retailers and other cash-system participants have needed repeated ACCC authorisations to discuss and develop industry responses to cash-in-transit sustainability and continuity risks, even where those discussions were directed to preserving public access to cash and financial-system resilience. A narrowly framed safe harbour could allow the RBA to convene, supervise and manage industry coordination on matters such as A2A migration, scam prevention, operational resilience, cryptographic uplift and cash access without each coordination process requiring a separate ACCC authorisation, provided the conduct occurs within written terms of reference approved by the RBA, is limited to public-interest coordination, excludes competitively sensitive pricing or customer allocation unless expressly authorised, and is subject to transparency, record-keeping and ACCC consultation safeguards. This would reduce procedural friction while preserving competition-law discipline for conduct outside the RBA-supervised process.

Finally, sequencing and coordination with the wider Treasury-led reform agenda, including PSP and payments licensing reforms, the SPF, the A2A roadmap through the Roundtable process, the AES migration program, and ongoing RBA and Treasury work on digital money, CBDC, tokenised asset markets and digital assets, is crucial to avoid fragmentation and duplication. Regulation should remain outcome-based and technology-neutral; governance and infrastructure decisions should align with the A2A roadmap and industry consultation outcomes; and new expectations should recognise the cumulative impact of overlapping initiatives on institutions' capacity to invest and innovate. Where issues fall partly outside the PSRA's formal scope, such as scam coordination across non-regulated entities, identity and digital security standards, or cross-border data sharing, the RBA can still play a constructive role through convening industry roundtables, guidance and collaboration with other authorities, including as Chair of the CFR and payments-specific coordination via the Payments System Modernisation forum established under the Government's Strategic Plan for Australia's Payments System.