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

Via email: pysubmissions@rba.gov.au

Dear Sir/Madam

Adyen Australia's submission to the Review of Payments System Regulation Issues Paper dated 25 June 2026

Adyen Australia Pty Limited ABN 55 162 682 411 (**Adyen Australia**, **we** or **us**) welcomes the opportunity to provide a submission in response to the Review of Payments System Regulation Issues Paper (**Issues Paper**) published by the Reserve Bank of Australia (**RBA**) on 25 June 2026.

Our submission responds to select aspects of the Issues Paper, focusing on competition across debit card networks, integrated platforms, tokenisation of card information, the use of AI agents in payments in e-commerce, the future of account-to-account payments, and fraud prevention.

About Adyen

Adyen (AMS: ADYEN) is the financial technology platform of choice for leading companies. By providing end-to-end payments capabilities, data-driven insights, and financial products in a single global solution, Adyen helps businesses achieve their ambitions faster. With offices around the world, Adyen works with the likes of Mecca, Lorna Jane, the Cotton On Group, Uber, H&M, eBay, and Microsoft. Adyen continuously improves and expands its product offering as part of its ordinary course of business.

Adyen is committed to the Australian market. Adyen Australia holds an Australian Financial Services Licence with the Australian Securities and Investments Commission and is registered as a reporting entity with the Australian Transaction Reports and Analysis Centre.

We look forward to our continued engagement with the RBA.

Yours faithfully,

SIGNED

Hayley Fisher
Country Manager, Australia and New Zealand
Adyen

Schedule 1

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?

Adyen offers its merchants least-cost routing (**LCR**) for both in-person and online transactions, alongside "Intelligent Payment Routing" (**IPR**) an AI-assisted tool that combines LCR with authorisation-rate optimisation to further reduce cost. In our experience, merchants prefer to have choice over their payments routing, implementing a balanced approach, not always deferring to the least cost option when it means a sale may not proceed.

The clearest source of durable, long-term competitive pressure on debit networks in mobile and online environments is a credible non-card alternative — account-to-account (**A2A**) payments via the New Payments Platform (**NPP**).

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?

As a global financial technology provider, Adyen supports a transparent, efficient and competitive payments landscape. We agree that transparency matters in helping merchants, particularly small and medium enterprises (**SMEs**), navigate the complexity of the payments industry. Greater transparency also supports merchants to make more informed decisions and even negotiate favourable commercial terms to their benefit.

However, we do not consider a lack of transparency to be the core issue currently limiting merchant choice. Integrated platform service providers compete on their verticalised software services, operational efficiency, service quality global capability, security, data insight, uptime and fraud prevention, in addition to cost — all markers of a genuinely competitive market. SMEs typically lack the time and specialised expertise to interpret the intricacies of payment pricing and interchange mechanisms regardless of how much is disclosed; integrated platform providers exist in part to bridge that gap. Layering further disclosure requirements onto merchants is therefore likely to yield diminishing returns.

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?

Competition within the integrated platforms market is not confined to price. Platforms compete on their software offering, operational efficiency, service quality (particularly authorisation rates), global capability, security, data insight, uptime and fraud prevention, in addition to cost — all markers of a genuinely competitive market.

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?

Adyen Australia strongly supports secure tokenisation and open token migration, and operates on an “open token” philosophy that does not impede merchants' ability to move between providers. We encourage others in the industry to adopt a similar approach, and do not see the need for further regulatory action at this point in time.

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?

Adyen Australia welcomes the growth of agentic commerce, which has significant potential to drive efficiency, product innovation and consumer benefit. As a member of the Agentic AI Foundation, Adyen is committed to a transparent, interoperable AI ecosystem that allows for open integration in the Australian market.

We submit that early-stage prescriptive regulation would be premature and could stifle innovation before use cases have matured. Instead, we recommend the RBA's initial focus be on fostering an open market that deters dominant technology and payment entities from siloing agentic infrastructure into closed commerce environments — monitoring the space closely while championing technical interoperability.

Where we do see a potential near-term role for policy is liability. What we see from our position — sitting between AI agents and enterprise merchants — is that the building blocks for agent identity, intent mandates and verifiable credentials are coming together. However, unlike in an entirely human-transaction flow, there is another surface area for a liability mismatch, whereby an agent acts outside of the consumer’s intent or misinterprets the parameters. The merchant received a legitimate payment. The bank processed a clean transaction. But the consumer is unhappy, and the chargeback framework was not built for this situation.

We recommend the RBA further consult with industry to help to assess how error-resolution and chargeback frameworks apply to agent-led payments and where there may be gaps.

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?

Adyen Australia recognises that A2A payments remain at an early stage of adoption in Australia, but see them as an important future source of competitive and innovative pressure — both directly, and as potential infrastructure for further developments such as agentic commerce.

The most significant structural challenge is interoperability and access to the NPP. As the RBA has itself noted, eligibility for direct participation favours authorised deposit-taking institutions (**ADIs**), with smaller institutions and non-bank PSPs facing substantial barriers to entry and relying instead on indirect connections. We recognise the short-term operational and compliance rationale for this restriction. However, we do not consider it should remain indefinite: we would encourage the RBA to set out a transparent, risk-based and time-bound roadmap toward broader direct-access eligibility for licensed non-ADI PSPs, rather than leaving the current restriction open-ended.

Separately, liability and dispute-resolution mechanisms that are well established for card payments remain underdeveloped for A2A payments. Chargebacks are effectively unavailable, leaving consumers to seek redress directly from merchants and placing additional strain on the Australian Financial Complaints Authority and the Australian Competition and Consumer Commission. We consider this a material constraint on both consumer trust and adoption, and address it further in our response to Question 12.

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?

The long-term growth of A2A payments requires a transparent, risk-based standard that narrows the gap between directly-connected ADIs and indirectly-connected non-bank participants, rather than leaving today's operational rationale as a permanent default.

On liability and dispute resolution, Adyen Australia recommends that the RBA support a dispute and liability framework to fill the vacuum of chargeback disputes. A standardised framework for payment reversals and dispute resolution is necessary for the long-term promotion of financial safety and mitigation of scam losses, in alignment with broader government priorities. The National Payments Corporation of India (**NPCI**), for example, has established a Unified Dispute and Issue Resolution (**UDIR**) framework for the Unified Payments Interface (**UPI**) to streamline dispute settlement between merchants and customers.

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?

A common obstacle to A2A adoption is customer friction. Cards and digital wallets remain dominant in user experience, offering a highly convenient and securely authenticated path for both in-person and (with autofill and saved credentials) online payments. A2A payments have historically required a manual process through a banking app at checkout, and this friction is a credible driver of drop-off and failed conversion. Deep-linking — pre-filling payment details via direct app-to-app redirection, as already implemented for India's Unified Payments Interface (**UPI**) and, in a more limited form, in the UK's open banking payment flows — can meaningfully reduce this friction.

On design, we would encourage the RBA to ensure any deep-linking or checkout-flow standard for A2A is developed with direct input from merchants and consumers on the resulting experience, not only from the participating financial institutions. The UK's early open banking payment flows are an instructive cautionary example: the initial bank-redirect experience was notoriously clunky, with significant drop-off, and took years of iteration — including the introduction of Variable Recurring Payments — to reach an experience that competes credibly with cards. Australia has the benefit of hindsight here and should not need to repeat that multi-year iteration cycle.

We would also note that chargebacks allow disputes over broader matters, such as receiving unsatisfactory goods, whereas A2A dispute mechanisms today address only technical payment errors — a further item for the RBA's consideration.

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

We consider standardisation and interoperability across cards and A2A payments best driven by industry bodies such as AusPayNet and Australian Payments Plus, with the RBA in an oversight and escalation role rather than as first-mover standard-setter. We would support the RBA formally endorsing the resulting standards once developed, to give them regulatory weight.

Q15–17: How is the payments industry strengthening its cryptographic practices in response to evolving cyber threats, what barriers do participants face, and what role could the RBA play in supporting industry-wide cryptographic uplift?

Adyen is a Principal Participating Organisation of the Payment Card Industry Security Standards Council (**PCI SSC**) and an active AusPayNet member, and supports the industry-led Advanced Encryption Standard (**AES**) Migration Program as the appropriate vehicle for cryptographic uplift in Australia's card payments system. We recognise the scale of this task — approximately 970,000 point-of-sale terminals and 25,000 ATMs require replacement or upgrade — and the genuine tension between competing near-term security investment and longer-term, more uncertain risks such as quantum computing, which the Australian Signals Directorate assesses could emerge as early as 2030.

We would encourage the RBA and AusPayNet to align guidance consistently with established international standards bodies — including the International Standards Organization, NIST, the IETF and the PCI SSC — so that participants across jurisdictions can work toward a single target state rather than reconciling divergent domestic and international timelines.

While we support RBA engagement, we do not consider direct regulatory intervention necessary or advisable at this stage. AusPayNet's contractual enforcement powers under the IAC Code Set already function as a quasi-regulatory mechanism for this migration, and duplicating that oversight through a parallel RBA framework risks adding operational complexity without a corresponding uplift in security. Should the RBA choose to engage further, we recommend a supportive role — providing resourcing and guidance aligned with AusPayNet's existing roadmap — rather than a parallel compliance regime.

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?

Card-not-present (**CNP**) fraud at overseas merchants is a genuine and growing problem: RBA data shows the value of CNP fraud on Australian-issued cards at overseas merchants grew from approximately $200 million to approximately $450 million between 2022 and 2025, and now accounts for around half of all fraud value on Australian-issued cards despite representing only around 3 per cent of transaction value — a gap the domestic CNP Framework, enforced through AusPayNet's IAC Code Set, does not reach because it does not extend to overseas merchants and acquirers.

As a global financial technology provider, we see this as a core risk in the payments landscape, and one we invest directly in addressing: our risk management suite, Adyen Protect, uses machine-learning models trained on network-wide, cross-merchant data to assess behavioural signals pre-authorisation and block fraudulent activity dynamically. Our most recent global fraud research shows the nature of the problem shifting even as tools improve — fraud losses associated with fraudulent chargebacks on our platform fell 20 per cent in 2025, but first-party fraud (where a customer disputes a legitimate purchase as unauthorised) is an increasingly common form of abuse reported by enterprises globally, ahead of fake accounts and identity abuse. This reinforces our view that fraud controls need to evolve with the threat, not simply intensify uniformly.

For that reason, we would caution against a blanket requirement for issuers to apply strong customer authentication (**SCA**) to all overseas CNP transactions. SCA in Australia already operates at a merchant/issuer-level under AusPayNet's CNP Framework — triggered where fraud exceeds defined thresholds under the IAC Code Set — rather than a scheme-level mandate, and we consider this targeted, threshold-based model more effective than a blanket rule. Merchants face real friction and conversion cost from additional authentication steps, and fraudsters routinely engineer workarounds to defeat rigid checkout controls — for example through one-time passcode subversion via social engineering, phishing or SIM swaps. We submit the RBA's focus is better directed at standardising issuer-level fraud controls specifically for overseas transactions, rather than introducing a new, separate blanket requirement.