Submission to the Reserve Bank of Australia's Review of Payments System Regulation Issues Paper

Tata Consultancy Services

7 August 2026

Table of contents

Note: sections under 'Detailed responses' align with those in the Issues Paper

A. Introduction

Tata Consultancy Services (TCS) recognises Australia's overarching agenda to modernise the payments system. Safely transitioning away from legacy infrastructure, such as the Bulk Electronic Clearing System (BECS) and paper cheques, is critical to fostering a dynamic, future-proof financial ecosystem.

TCS brings deep global expertise across the payments ecosystem, helping banks, payment providers, central banks and merchants modernise payment infrastructure and deliver secure, real-time payment services.

Through our TCS BaNCS™ platform and extensive consulting capabilities, TCS supports domestic and cross-border payments, real-time payments, card processing, merchant payments, direct debits and payment operations.

TCS has experience supporting payment systems in 25 countries and more than 40 clearing networks, enabling clients to improve efficiency, strengthen resilience, meet evolving regulatory requirements and accelerate innovation.

TCS is also recognised for our experience in designing and operating large-scale national payment infrastructures, in particular as a key technology partner behind India's Unified Payments Interface (UPI), one of the world's largest real-time payment networks. This is an example of common infrastructure supporting rapid digital payment adoption, with retail digital payments growing 100-fold from FY2012-13 to FY2023-24 (RBI Payment System Report, December 2024). In H2 2025, UPI represented 85% of India's digital-payment transaction volume, while accounting for 9.1% of transaction value, demonstrating its role as a high-volume retail rail alongside separate high-value infrastructure. (RBI Payment System Report, June 2025)

Drawing on this experience, TCS advises governments, regulators and financial institutions on payment modernisation, interoperability, fraud prevention and account-to-account payment models.

In Australia, TCS has supported the Reserve Bank of Australia's banking and payments capabilities through the deployment of the TCS BaNCS platform and related cloud transformation initiatives. See the final section for more detail.

B. Our perspective

TCS welcomes the opportunity to respond to the Review of Payments System Regulation Issues Paper.

1. Over-arching approach to Australia's ecosystem

We view Australia's payments system as three connected layers.

The first layer is core payment infrastructure, including the Reserve Bank Information and Transfer System (RITS), the New Payments Platform, BECS, eftpos and major card payment networks.

The second layer is governance and access. This includes access rules, technical standards, routing, fee transparency, participation rules and coordination between market participants.

The third layer is innovation and customer services. This includes digital wallets, Buy Now Pay Later (BNPL), PayTo use cases, merchant platforms, embedded finance, fraud tools, loyalty services and new commerce models.

The practical principle should be simple: the closer the function is to core infrastructure, the stronger the case for RBA oversight. The closer a function is to customer-facing innovation, the stronger the case for market-led competition, supported by clear safeguards.

Three-layer approach

Layer	RBA focus	Competition impact	Efficiency and safety impact
Core infrastructure	Resilience, settlement safety, interoperability and stability of critical participants.	New entrants can use reliable rails instead of rebuilding them.	Reduces systemic risk and keeps payments flowing.
Governance and access	Fair access, transparent rules, effective routing and fee disclosure.	Reduces barriers and gives merchants real choice.	Reduces friction, switching costs and hidden dependency risks.
Innovation and customer services	Disclosure, consumer protection and operational accountability.	Allows firms to compete on product, price and service.	Encourages investment while managing scams and conduct risks.

1. Core payment infrastructure
The RBA should give highest priority to the core infrastructure layer. This layer supports daily payments by households, businesses and government. It also supports confidence in the financial system.

The RBA already oversees systemically important and prominent payment systems because disruption in these systems could affect the economy. The key priorities should be operational resilience, cyber security, settlement finality, business continuity, interoperability and fair access to essential payment rails. This promotes financial security because it reduces the risk of system-wide disruption, promotes efficiency as payments can move reliably and at scale, and promotes competition because new providers can access core rails on fair terms.

The RBA should also consider the stability of critical participants in this layer. A major outage or distress event at a settlement participant, infrastructure operator, scheme operator, gateway or processor could disrupt payments even if the payment rail itself is still working.

This does not mean the RBA should become the prudential regulator of all payments participants. Rather, the RBA should monitor critical dependencies. It should expect recovery plans, continuity plans and stress-event playbooks for entities whose failure could affect the wider payments system.

2. Governance and access
The second layer is where the RBA can have a strong effect on competition, which is affected by more than interchange fees. Competition is also affected by scheme rules, wallet access, merchant service fee transparency, least-cost routing, technical standards and the ability of merchants to switch providers.

The RBA should focus on fair access, open standards, clear participation rules and transparent pricing. These measures help merchants and new entrants compete on merit. The RBA should not try to choose commercial winners. It should remove unnecessary barriers and make sure that rules are fair, transparent and practical.

This would improve competition by reducing entry barriers, improve efficiency by reducing avoidable switching costs and processing friction, and improve financial security by reducing hidden concentration and dependency risks.

3. Innovation and customer services
The third layer should mainly be market-led. This layer includes digital wallets, BNPL, PayTo-based services, merchant software platforms, embedded finance, fraud tools, loyalty services and emerging models such as agentic commerce. This is where competition and innovation can bring the greatest benefit to consumers and merchants.

Heavy regulation of this layer could reduce innovation, slow investment and protect existing players. At the same time, there should be clear expectations on transparency, consumer protection, fraud controls, operational accountability and fair disclosure of costs and risks.

The better model is outcome-based regulation. Regulators should define the outcomes expected. Market participants should then compete on product design, technology, pricing and service quality.

For example, UPI has 3 three layers, with innovation in the outer layer. Players like Google and Phonepay have developed a mobile app for UPI payments with features such as:

- paying through contact number in the handphone instead of account number or email, and the payment is initiated in handphone,
- offer transaction history,

- checking bank balance
- credit score
- bill payments
- applying for loans

It is worth noting that the payments system operator (NPCI) also developed its own mobile app but did not offer the above features. This underlines that the innovation layer should be led by market forces and the regulator should only have limited oversight of this layer.

C. Detailed responses

We have chosen to provide selective, detailed response to the questions posed in the paper, focusing on those topics where we have global expertise to share. Where relevant, we have shared insights from our pivotal role as a key technology partner behind development of India's Unified Payments Interface (UPI).

Section 2.2: Integrated platforms and bundling of payment services

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?

Difficulty of switching
The difficulty of switching away from an integrated platform services provider to access a preferred payment service provider (PSP) varies significantly across merchant segments. For merchants using standard e-commerce integrations, switching may be relatively straightforward. However, for merchants that have adopted deeply integrated platform solutions incorporating payments, subscription management, fraud prevention services, reporting, reconciliation and customer management functionality, switching can be materially more complex.

Switching costs increasingly arise from operational and technical dependencies rather than contractual lock-in. These costs may include integration redevelopment, testing and certification, migration of recurring payment arrangements, replacement or remapping of tokenised payment credentials, changes to reporting processes, staff retraining and temporary business disruption.

This is particularly relevant in the context of the Reserve Bank's Least Cost Routing objectives. The RBA has consistently emphasised that merchants should be able to benefit from competition between payment providers and routing options, particularly for dual-network debit card transactions. Where platform design, technical architecture or commercial arrangements make switching PSPs difficult, merchants may be less able to exercise effective choice over payment acceptance arrangements.

Adequacy of pre-contract information
In our view, merchants generally receive adequate information regarding transaction pricing, onboarding requirements, settlement arrangements and core contractual terms before joining an integrated platform.

However, the information provided is often less comprehensive regarding the practical implications of switching PSPs after implementation. Merchants may not always receive clear and easily comparable information regarding:

- The cost and effort required to migrate to an alternative PSP.
- Whether network tokens, stored credentials and recurring payment arrangements can be transferred to another provider.
- Additional charges associated with connecting a third-party PSP.

- Functional differences between the platform's preferred PSP and alternative PSPs.
- The impact that PSP choice may have on routing flexibility and LCR outcomes.
- Expected implementation timelines and business disruption associated with migration.

Consequently, while merchants are generally able to assess the cost of entering an integrated platform ecosystem, they may have a less complete understanding of the potential cost, complexity and operational risks associated with exiting that ecosystem.

Areas for increased transparency
Greater transparency would enable merchants to make more informed decisions on both platform selection and payment provider choice. To improve transparency, integrated platform providers should disclose, in a standardised and easily understandable format:

- Any fees or commercial consequences associated with using a PSP other than the platform's preferred provider.
- Whether tokenised payment credentials and recurring payment arrangements can be migrated to another provider and any limitations that may apply.
- Expected migration effort, implementation timelines and support obligations.
- Any material differences in functionality, reporting, fraud tools, checkout capabilities or customer experience available to alternative PSPs.
- Whether the merchant's ability to access routing options, including LCR functionality where relevant, may be affected by platform design or PSP selection.

Such disclosures would allow merchants to better assess the total economic impact of platform selection, rather than focusing solely on upfront pricing and onboarding considerations.

Alignment with Regulatory Objectives
From a policy perspective, the primary issue is not whether integrated platforms should offer embedded payment services. These solutions often deliver significant efficiencies for merchants and can accelerate digitisation of small and medium businesses.

Rather, the question is whether merchants can continue to exercise effective and informed choice over PSP selection throughout the life of the relationship.

Improved transparency regarding switching costs, token portability, third-party PSP access and routing flexibility would support the RBA's longstanding objectives of promoting competition, efficiency and merchant choice within the payments system. This approach is also consistent with the broader direction of regulatory developments internationally, including initiatives focused on interoperability, portability and reducing barriers to switching in digital ecosystems – as seen in the EU's Digital Markets Act and Data Act, and the UK's Digital Markets, Competition and Consumers (DMCC) Act .

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?

There are well known examples where regulators have had to deal with uncompetitive bundling in both the payments sector and other sectors.

For instance, Apple bundled payments into its App Store, forcing developers to use its in-app purchase system and blocking cheaper outside options. In response, regulators did not ban the store. The Netherlands ACM, the EU Digital Markets Act, and the US Epic v. Apple ruling instead forced Apple to allow external payment providers on fair terms.

In Australia, carmakers bundled vehicles with proprietary repair data, releasing it only to authorised dealers and shutting out independent mechanics. Rather than ban manufacturer servicing, the Motor Vehicle Information Scheme, mandatory since July 2022, requires makers to share repair data with all repairers at fair market value through a neutral industry-led body.

Similarly, bundling payments inside integrated platforms raises competition and efficiency issues, and a lesser financial safety issue. But the solution is not to ban bundling or cap platform fees. Instead, terms should be clear to merchants before they sign and it should be easier for them to switch. The RBA can do most of this with tools it already holds. It should leave conduct to the ACCC and provider safety to the new licensing regime.

We do not propose that the RBA limit the depth of the relationship between an acquirer and a merchant. Deep, valuable relationships, built on better settlement, lending, routing and service are good for competition and should be encouraged. The issue is when relationships are held together by the cost of leaving rather than the value of staying. The remedies we set out below target the switching cost, not the relationship.

Competition: a switching problem, not a bundling problem
Integrated platforms bring business software and payment acceptance together in one place. This is convenient for small merchants. The problem starts when the platform makes it hard to use a different payment provider. It can charge a penalty fee for using an outside provider, make the outside checkout slower, or make its own option the easy default. The result is weak competition at the point where a merchant chooses who processes their payments.

This matters more now. With the removal of surcharging from 1 October 2026 competition is meant to move onto the fees that providers charge merchants. If a merchant cannot easily move to a cheaper provider inside their platform, that new competition never reaches them. In effect, bundling can cancel out the benefit of reforms the RBA has just delivered.

Impact on least-cost routing
Bundling lowers the cost of getting started, with one sign-up, one bill and fraud tools built in. The cost to merchants and consumers shows up later. Least-cost routing works well in person, at about 76 per cent of merchants at the end of 2024 according to the RBA, but is “at a much earlier stage” online and in mobile wallets. Integrated platforms sit right in that online gap. Where the platform controls the checkout, the merchant often cannot send dual-network debit down the cheaper network.

Financial safety considerations
Financial safety does not threaten the stability of the financial system. However, there is a real risk that if a platform fails, is breached, or offboards a merchant, the merchant can lose the tokenised card details and recurring billing set up inside that platform and may be unable to keep taking payments. Safeguarding of merchant money and provider resilience are already being handled through the Treasury *Payment Systems Modernisation* reforms so the RBA’s role here should focus on token portability.

We recommend that the following actions are considered:

1. **Extend least-cost routing expectations to online and integrated platforms.** The RBA already expects providers to offer and promote LCR. It should say clearly this applies inside integrated platforms and in-app checkouts, not only at the terminal.
2. **Make network tokens portable, delivered through a neutral, industry-governed layer.** A merchant should be able to move their tokenised card details and recurring mandates to a new provider without asking customers to re-enter their cards. The cleanest way to deliver this is a neutral token layer, where tokenised credentials are mapped to the merchant rather than held by the incumbent provider. Switching acquirer then simply re-points that mapping. Customers do not re-enter cards, recurring billing keeps working, and the main barrier to switching falls away. The most credible steward for this layer is Australian Payments Plus (AP+), which already operates eftpos and sits at the centre of domestic payments infrastructure. A neutral layer, governed by industry and sitting inside the new licensing regime, would give merchants genuine choice and let the better performing acquirer compete for a merchant's business on merit. It would also avoid the worse outcome of creating a new private monopoly over the nation's recurring-billing credentials. We put AP+ forward as a potential home, not the only option, and we would support the RBA testing this with industry.
3. **Require a plain pre-contract switching disclosure.** Before a merchant signs, the platform should disclose, in a standard form, any penalty for using an outside provider, whether routing is available, and whether tokens can be taken on exit.
4. **Refer self-preferencing and fee conduct to the ACCC, not the RBA.** Penalty fees, self-preferencing and unfair terms are competition and consumer matters. The ACCC has already documented switching costs and weak transparency across digital platforms. The RBA should coordinate rather than duplicate.

Section 2.3: Tokenisation of Card Information

> 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 set a token portability expectation in December 2023, asking schemes, gateways and acquirers to support portability by the end of June 2025 to ease merchant switching. The industry responded, and AusPayNet approved a merchant data porting standard in May 2025. However, that standard carries a 12-month transition, so full compliance is not expected until around mid-2026 — about a year after the RBA's original date. The industry cited technical sequencing dependencies for the delay.

In our view, the deeper issue is that an 'expectation' is a soft instrument and moves at the pace of the least-willing participant. The lesson is that portability is unlikely to arrive promptly through expectations alone. The RBA should therefore (a) convert the portability expectation into an enforceable standard under the amended PSRA, and (b) ensure it explicitly captures tokens held inside integrated platforms, delivered through a neutral steward such as AP+.

Regulatory intervention should be proportionate and focused on preventing merchant lock-in, preserving LCR, strengthening data security and ensuring that tokenisation does not become a mechanism for scheme or provider-level competitive advantage.

The following actions should be considered:

- **Mandated Token Portability Standards:** Require schemes, acquirers, gateways and PSPs to support a common, operationally tested token migration framework for both scheme and proprietary tokens. The standard should define timelines, roles, data fields, exception handling, liability treatment and customer notification requirements so that merchants can switch providers without forcing customers to re-enter card credentials.

- **Token Synchronisation and PAR Usage:** Mandate the use and sharing of a unique account identifier such as PAR across relevant participants, subject to privacy and security controls. This will help ensure that multiple tokens linked to the same account are updated consistently when issuer-held credentials change, reducing failed transactions and improving efficiency.

- **DNDC and Least-Cost Routing Protection:** Require that tokenisation of dual-network debit cards (DNDC) supports both domestic and international network tokens where available, unless a merchant makes an explicit choice otherwise. This is essential to ensure tokenisation does not weaken merchant routing choice or reduce competitive pressure on scheme fees.

- **PAN Storage Controls and Compliance Monitoring:** Apply a clear compliance framework for merchants and PSPs that continue to store PANs, aligned at minimum to PCI DSS. The RBA should consider periodic attestation, reporting and supervisory review for larger participants or those holding significant volumes of card-on-file credentials.

- **Industry Reporting and Transparency:** Introduce periodic industry reporting to track token portability readiness, migration volumes, failed migration rates, synchronisation performance and unresolved technical barriers. Transparent monitoring will allow the RBA to identify whether expectations are working in practice or whether enforceable standards are required.

Overall, the RBA's tokenisation expectations are directionally sound and have helped align the industry around security, portability and competition outcomes. However, given the multi-party dependencies and the risk of provider lock-in, the RBA should closely monitor implementation and be ready to introduce enforceable, outcome-based requirements if voluntary coordination does not deliver practical portability and synchronisation across the card payments ecosystem.

Section 2.4: Use of AI agents for payments in e-commerce

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?

AI agents can improve e-commerce checkout efficiency, fraud detection and consumer convenience, but they also create a new control point between consumers, merchants, wallets, schemes and PSPs.

We see at least three key areas of risk:

- **Competition risk:** Agents may default to the rail preferred by a platform, wallet, scheme or model provider rather than the lower-cost eligible rail. This could weaken merchant choice and replicate routing frictions already observed in online and mobile-wallet environments.

- **Efficiency risk:** Agentic checkout can reduce friction, but closed protocols, opaque fee layers and limited interoperability could create regulatory asymmetry and cross-subsidisation in favour of proprietary ecosystems.

- **Financial safety risk:** Delegated authority creates ambiguity around consumer intent, authentication, fraud, mistaken purchases, chargebacks and liability allocation between the consumer, merchant, PSP, wallet, platform, agent provider and scheme.

The RBA should respond proportionately by preserving merchant choice, making payment selection observable, clarifying consent and liability, and bringing agentic payment actors within the regulatory perimeter where they materially influence payment initiation or routing.

We recommend that the RBA take a risk-based, technology-neutral and evidence-led approach based on the following principles:

- **Clarify the perimeter:** Treat an AI agent, wallet, gateway or platform as relevant to payments regulation where it initiates, influences, prioritises or routes a payment method.

- **Preserve merchant choice:** Require agent-influenced transactions to support merchant routing choice and least-cost routing where technically feasible, commercially relevant and authorised by the consumer.

- **Mandatory transparency:** Require merchants to see the rail used, routing logic category, additional agent/platform fees and whether a lower-cost eligible rail was available.

- **Setting consent and authority controls:** Require explicit consumer mandates, spending limits, revocation rights, strong authentication, pre-execution prompts for higher-risk transactions and tamper-evident audit logs.

- **Allocate liability and dispute rights:** Define responsibility for unauthorised, erroneous, manipulated or agent-misinterpreted transactions across consumers, merchants, PSPs, wallets, platforms and agent providers.

- **Create reporting and monitoring:** Add agent-initiated payment data to retail payments reporting, segmented by card, account-to-account, wallet, BNPL and other rails, including whether routing choice was available.

This approach is consistent with the global direction of travel: the UK's Financial Conduct Authority (FCA) favours outcomes-based use of existing frameworks for AI; the Bank of England/FCA AI work highlights governance, consumer outcomes, third-party risk and operational resilience; and the Monetary Authority of Singapore (MAS) points to board oversight, AI inventories, lifecycle controls, human oversight, testing and monitoring, including for AI agents. In Australia, this should be anchored in the RBA's focus on merchant choice, account-to-account payments, mobile wallets, cryptography and fraud prevention, and its established LCR policy work.

Section 4.1: Future of Account to Account Payments

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 the RBA to consider proportionate regulatory action in relation to A2A payments. Given the scale of existing A2A payments, gaps in access, interoperability or resilience could have broader implications for the financial system.

Regulatory action may be warranted in the following areas:

- **Access and participation:** The RBA could consider measures to promote fair, transparent and risk-based access to A2A payment systems for smaller institutions and non-bank payment service providers. This may include clearer access criteria, transparent onboarding processes, reasonable timelines, and oversight of direct and indirect access arrangements. For instance, in India medium and large banks are provided direct member access to the primary electronic funds systems (NEFT, RTGS and IMPS) whereas smaller banks are provided sub-member access with clearly defined policies of onboarding and settlement. Some 90-95% of around 22 billion transactions per month are initiated in apps provided by non-banking institutions.

- **Interoperability and standardisation:** The RBA could support or mandate appropriate technical, operational and messaging standards across A2A payment systems to improve interoperability. This would help reduce complexity, lower entry barriers, support innovation, and enable payment providers to re-route or fail over transactions during disruptions. In India, there are two real-time payment railroads (UPI & IMPS) that provide PSPs the option to re-route from one to another as they follow the same standards, albeit with proprietary specifications. This also helps in distribution of load across systems.

- **Operational resilience and risk management:** The RBA could establish minimum resilience, availability, incident management and continuity requirements for critical

A2A payment infrastructure. This would help control risks to the financial system and maintain confidence in essential payment services.

- **Competition safeguards:** The RBA could monitor whether existing ownership, governance or access arrangements create barriers to competition or innovation. Where necessary, it could consider regulatory requirements to ensure that dominant participants or infrastructure providers do not restrict access or favour providers.

- **End-user protection and consistency:** The RBA could promote minimum service standards for A2A payments, including reliability, transparency of payment timing, clear dispute or error-handling processes, and consistent end-user experiences across institutions.

Any regulatory intervention should be targeted, proportionate and risk-based. The RBA should avoid excessive standardisation that could restrict innovation or prevent providers from offering differentiated services. A balanced approach would be to use regulation to establish minimum public-interest requirements—particularly around access, interoperability, resilience and safety—while allowing industry participants to innovate and compete above those baseline standards.

Section 4.2: Competition between Cards and A2A payments

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

The RBA should take targeted regulatory action. Australia already has the rails (NPP), the mandate layer (PayTo), and, from 1 October 2026, a surcharge ban that finally makes a fee-free alternative to cards attractive to merchants (RBA Conclusions Paper, March 2026). The missing piece is a shared front door — an open acceptance standard, starting with QR — that lets cards and A2A compete at the checkout. In our view, closing that gap is the highest-leverage action in this review.

The core problem is the missing QR layer. NPP was built for account-to-account transfers, not point-of-sale. PayTo is still a small share of NPP volume and mostly used for subscriptions and bills, not shop-front payments (Azupay). QR payment exists in Australia but only as closed loops (QwikPay, Wpay, café apps), each needing merchant and customer on the same private scheme. There is no open “scan any QR with any bank app” like India’s UPI. The timing is critical: the surcharge ban shifts card costs onto merchant margins and BECS is being retired with the future of A2A only now being defined (RBA Issues Paper §4).

In response, the RBA should back an open, interoperable QR standard. AP+ already aims to “enable in-store payments using any smart device, initially via QR” (AP+ Roadmap). The RBA should set the public interest guardrails with one common QR standard, open to all banks and PSPs. In India, for example, a RuPay credit card and a bank account now ride the same UPI QR, and the customer chooses at payment (NPCI). As a result, credit acceptance went from under 10 million card terminals to over 50 million QR merchants (Economic Times).

The RBA should set common messaging standards, not develop product. Baseline ISO 20022 and acceptance standards so card and A2A are presented consistently across wallets, checkouts and terminals. It should analyse wallet and device choke points by assessing whether NFC, wallet and operating-system rules stop A2A competing with cards at the tap point. The foundation should be competitive neutrality. No standard should tilt the field toward cards or A2A; rails compete on cost, speed, security and experience. Resilience should come through a shared acceptance layer that lets merchants fail over between rails during outages — a financial-safety gain, not just competition. And safety must be a pre-condition. A2A payments are near-final with no chargeback, widening the scam surface. Confirmation of Payee (live at ~80 institutions) and strong authentication must be prerequisites (AP+).

Australia does not need new rails. It needs a shared, neutral and safety-gated front door for its existing rails. AP+ and the A2A Roundtable should deliver the standard but signal that if it is not delivered to timeline, it will move to an enforceable standard under the amended PSRA. The RBA's own least-cost-routing experience shows expectation timelines slip when they rely on participants who benefit from the status quo (RBA, Least-cost Routing). Done well, this turns A2A from a bills rail into a genuine competitor to cards, letting consumers choose account or card in a single flow.

Section 5.2: Card Payments Fraud Overseas

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?

We suggest that the RBA consider a targeted regulatory response if current industry-led arrangements are not sufficient to reduce overseas card-not-present (CNP) fraud affecting Australian-issued cards. The response should recognise that the RBA cannot directly regulate all offshore merchants and acquirers, but it can influence domestic participants, card schemes and acceptance arrangements that enable Australian cards to be used in high-risk overseas environments.

The following regulatory actions should be considered:

- **Scheme-Level Accountability:** Require international card schemes operating in Australia to demonstrate how they manage overseas CNP fraud on Australian-issued cards, including merchant monitoring, high-risk acquirer oversight, fraud-rate thresholds, and enforcement actions for offshore participants with persistent fraud issues.

- **Risk-Based Authentication Standards:** Encourage or require stronger authentication for high-risk overseas CNP transactions, including greater use of 3-D Secure, tokenisation, device intelligence, behavioural analytics and risk-based step-up authentication. The requirement should be designed to reduce fraud without creating unnecessary friction for low-risk legitimate transactions.

- **Issuer Controls and Customer Choice:** Support clearer issuer-level controls that allow cardholders to manage overseas online transaction capability, including opt-in/opt-out controls, transaction limits, merchant-category restrictions and real-time alerts. These controls should be easy to use and should not unfairly shift responsibility to consumers for sophisticated fraud.

- **Fraud Data Reporting and Transparency:** Mandate more granular reporting of overseas CNP fraud by geography, merchant category, scheme, transaction type, authentication status and tokenisation status. Better transparency would help the RBA, issuers and schemes identify systemic vulnerabilities and target interventions efficiently.

- **Liability and Incentive Alignment:** Review whether liability rules appropriately allocate losses to the parties best placed to prevent fraud. Where offshore merchants, acquirers or schemes do not apply adequate authentication and fraud controls, the liability framework should create incentives for stronger prevention rather than simply passing losses back to Australian issuers and consumers.

- **International Coordination:** Work with overseas regulators, card schemes and industry bodies to promote consistent baseline controls for cross-border CNP transactions. Given the international nature of the threat, regulatory expectations should be aligned where possible with global authentication, tokenisation and fraud-monitoring standards.

Overall, the RBA should consider a proportionate, outcome-based response focused on scheme accountability, stronger controls for high-risk cross-border transactions, improved transparency and better alignment of liability. This would support financial safety while preserving competition and efficiency in legitimate cross-border card payments.

Next steps

We would be pleased to facilitate further discussions for the RBA with payments experts within the TCS global network. We would also be pleased to host RBA officials if they intend to undertake a study visit to India.

C. TCS and the RBA

Tata Consultancy Services (TCS) is a global leader in IT services, consulting, and business solutions, maintaining deep practices in financial services and national payments infrastructure. As the core technology partner to the National Payments Corporation of India (NPCI), we helped design, build, and continue to secure the UPI ecosystem, which processes billions of transactions monthly.

TCS has a long-standing and valued partnership with the Reserve Bank of Australia. We have worked closely with the RBA to deploy the TCS BaNCS Core Banking solution so that the RBA can provide banking services to the Australian Government. We have also worked with the RBA to migrate all applications, including BaNCS, to the Azure cloud.