



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

Table of Contents

Table of Contents	2
Group Country Manager Letter	3
Executive Summary.....	4
Overview	6
Issues for Consultation.....	9
Merchant Choice in Payments	9
Competition across debit card networks	9
Tokenisation of card information.....	11
Use of AI agents for payments in e-commerce	12
Mobile Payments, Non-designated Card Networks and Buy Now Pay Later.....	16
Non-designated card networks	16
Account-to-account Payments.....	17
Future of account-to-account payments	17
Competition between cards and account-to-account payments	18
Cryptography and Fraud Prevention.....	20
Cryptography in the payments system	20
Card payments fraud overseas.....	24
About Visa	28

Group Country Manager Letter

21 August 2026

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

Via email: pysubmissions@rba.gov.au

Dear Ellis,

Visa's submission to the Reserve Bank of Australia's Review of Payments System Regulation – Issues Paper

Visa welcomes the opportunity to respond to the Reserve Bank of Australia's (RBA, the Bank) Issues Paper as part of its Review of Payments System Regulation (the Review).

Since the early 2000s, we have appreciated the ongoing dialogue with the RBA on Australia's digital payments ecosystem and Visa's role to promote safe, secure, and convenient payments that benefit all Australians. Visa has engaged with the RBA on a wide range of reviews and consultations during this period.

As with each previous occasion, we are grateful for the opportunity to share our perspectives, emphasising the importance of approaching digital payments with a focus on the guiding principles of consumer and merchant choice and protection, security, and continuous innovation, within the framework of a level playing field.

Visa remains strongly committed to working collaboratively with the RBA and we would welcome engaging further with the Bank ahead of the Review's conclusion – in the spirit of a joint effort to continue building a digital payments system that supports Australia's economic ambitions and delivers secure, efficient, and inclusive outcomes for all.

Yours sincerely,



Alan Machet
Group Country Manager
Australia, New Zealand and Pacific Islands

Executive Summary

- **The Review presents an important opportunity to address the longstanding regulatory asymmetry between designated four-party and three-party networks, particularly American Express.** Since the early 2000s, the RBA has recognised that three-party networks compete directly with four-party networks for merchant acceptance, while reserving the right to reassess their treatment as market dynamics evolved. Those dynamics have now materially changed.
- **The Payments System Modernisation Act has clarified that three-party and closed-loop networks fall within the regulatory perimeter of the Payment Systems (Regulation) Act 1998 (PSRA).** The question is, therefore, no longer whether the RBA has the power to act, but whether continued regulatory asymmetry remains consistent with the public interest.
- As the RBA observes, the use of AI agents in e-commerce is a rapidly developing area. In light of this, **it is critical to ensure sufficient investment for the future of payments and commerce in a way that help protect Australia's ability to capture the productivity dividend that agentic commerce offers.**
- **The safety and resilience of Australia's payments system also require continuous, long-term investment in cybersecurity infrastructure and effective fraud prevention.** The payments industry is strengthening its cryptographic practices through a combination of coordinated industry migration programs, adoption of stronger cryptographic standards, and preparation for future threats associated with quantum computing.
- **Overseas card-not-present (CNP) fraud remains an important financial safety issue** for the Australian payments ecosystem, particularly given the cross-border nature of the risk and the more fragmented control environment that applies to overseas merchants, acquirers, and service providers. However, **any assessment of whether additional regulatory intervention is required should be guided by current fraud outcomes and the effectiveness of existing controls.**
- Visa supports the recently published vision for Australia's account-to-account (A2A) payments system.¹ Action to achieve this vision should **ensure that consumers and merchants can choose between cards, A2A, or other payment methods with a clear understanding of the protections, value, and operational implications of each.**
- **Visa supports preserving the RBA's approach to date on Least Cost Routing (LCR), in this case for the online and mobile channels.** This allows merchants to consider factors, such as authorisation rates, platform technology, security, value-added services, data and analytics capabilities, system resilience, innovation, and convenience, when making routing decisions.

¹ A2A Payments Roundtable (2026), [Vision for Australia's A2A payments system](#).

- **Visa supports industry participants adopting token portability, synchronisation, and visibility based on their role in the ecosystem.** These capabilities are available through Visa's network tokenisation program and support a robust, competitive ecosystem.

Overview

Visa shares the Government's ambition to build a secure and trusted payments system that drives competition, innovation, and productivity across Australia's economy. As the Assistant Treasurer and Minister for Financial Services, Daniel Mulino, observed upon the recent passage of the Payments System Modernisation Act, "a safer, more trusted and more accessible payments system will help boost competition, innovation, and productivity across the economy."² The Government's Strategic Plan for Australia's Payments System likewise places productivity at the heart of its vision for a "modern, world-class, and efficient payments system that is safe, trusted, and accessible."³ Australia's payments system, and the regulatory settings that govern it, will either be a critical enabler — or constraint — on whether that potential is realised.

The RBA's Review of Payments System Regulation, therefore, is taking place at a pivotal moment. As the Issues Paper notes, the payments landscape is being reshaped by significant innovation and structural change.⁴ Visa shares the RBA's assessment that a well-functioning payments system is characterised by strong contestability, effective interoperability, and appropriate standardisation — features that support entry and expansion by participants, enable end users to choose and switch between providers, and facilitate innovation.⁵ It is precisely these characteristics that Visa's submission seeks to protect and strengthen.

The RBA has identified a broad range of issues within the Issues Paper. Of these, Visa considers that there are a select few that are critical to ensuring a well-functioning payments system and, therefore, warrant the RBA's focused action in this Review. Visa identifies three such critical issues:

1. Addressing the regulatory asymmetry that continues to undermine competitive neutrality between three- and four-party networks;
2. Maintaining sufficient value within the payments system, which is critical to ensure participants have an enduring economic incentive to invest in future capabilities, including fraud prevention, cybersecurity, and emerging technologies, such as quantum computing, cryptographic resilience, and agent commerce; and
3. Ensuring informed consumer and merchant choice across cards, account-to-account (A2A), and other payment methods, recognising that these carry materially different protections, costs, and liability frameworks.

Competitive neutrality between three- and four-party networks

The Review presents an important opportunity to address the longstanding regulatory asymmetry between designated four- and three-party networks, particularly American Express. Since the early 2000s, the RBA has recognised that three-party networks compete directly with

² Treasury (2025), [Reforms to modernise Australia's payments system pass the Senate](#).

³ Treasury (2023), [A Strategic Plan for Australia's Payments System](#), p1.

⁴ Reserve Bank of Australia (2025), [Review of Merchant Card Payment Costs and Surcharging Consultation Paper](#), p3.

⁵ Ibid.

four-party networks for merchant acceptance, while reserving the right to reassess their treatment as market dynamics evolved.⁶ Those dynamics have now materially changed.

The Payments System Modernisation Act has clarified that three-party and closed-loop networks fall within the regulatory perimeter of the PSRA. This reflects Parliament's clear intent that the RBA has the authority to regulate a broader range of participants and payment networks where necessary to promote competition, efficiency, and financial safety.⁷ The question is, therefore, no longer whether the RBA has the power to act, but whether continued regulatory asymmetry remains consistent with the public interest.

Maintaining sufficient value within the payments system

The Government has made Artificial Intelligence (AI) a central priority of its productivity agenda. Treasurer Chalmers has described AI as “a game changer for our economy”⁸ and the 2026-27 Budget productivity package explicitly positions AI as foundational to delivering the economic gains identified by the Productivity Commission.⁹ In Visa's view, agentic commerce – where AI agents discover, compare, and complete purchases autonomously on behalf of consumers – is the payments system's most direct manifestation of this opportunity.

As the RBA observes, the use of AI agents in e-commerce is a rapidly developing area.¹⁰ Visa approaches this transition as an active participant to enable innovation to scale safely. Just as Visa's investment in contactless capabilities and tokenised mobile wallets helped Australia emerge as a global leader in those technologies, we are today constructing the foundations for innovative, secure, and trusted agentic commerce, through solutions and programs such as Visa Intelligent Commerce, the Trusted Agent Protocol, and the Agentic Ready Program that will usher in the next generation of merchant opportunities.¹¹ Against this backdrop, it is critical to ensure sufficient investment for the future of payments and commerce in a way that helps protect Australia's ability to capture the productivity dividend that agentic commerce offers.

The safety and resilience of Australia's payments system also require continuous, long-term investment in cybersecurity infrastructure and effective fraud prevention. Between 2020 and 2025, overall Visa card fraud rates in Australia fell by approximately 28 per cent, while both domestic and cross-border CNP fraud rates declined by about 40 per cent, reaching their lowest levels in the past six years.¹² This reduction has been achieved through significant investments, particularly regarding layered network-level controls, tokenisation, and authentication. Such investments are increasingly vital in the context of the rapidly evolving threat environment – and will be even more so in the future.

⁶ Reserve Bank of Australia (2005), [Payments System Board Annual Report – 2005 | Credit and Charge Cards](#); Reserve Bank of Australia (2001), [Designation of Credit Card Schemes in Australia](#).

⁷ Parliament of Australia (2025), [Treasury Laws Amendment \(Payments System Modernisation\) Bill 2025 Second Reading](#).

⁸ Treasury (2025), [The Hon Dr Jim Chalmers MP - Press conference, Canberra](#).

⁹ Treasury (2026), [Budget 2026-27 Productivity Package](#), p6.

¹⁰ Reserve Bank of Australia (2025), [Review of Merchant Card Payment Costs and Surcharging Consultation Paper](#), p3, 11.

¹¹ Visa (2026), [Visa Welcomes Partners into Agentic Ready Program to Unlock Agentic Commerce](#).

¹² Visa Fraud Reporting.

Looking ahead, quantum computing presents a medium-term but material threat to the cryptographic standards underpinning the entire payments system. Maintaining a regulatory framework that preserves the economic incentive supporting fraud prevention, cybersecurity, and cryptographic resilience will be critical to maintaining the economic incentives that underpin innovation across the payments system.

Ensuring informed consumer and merchant choice across cards, account-to-account (A2A), and other payment methods

Visa supports the recently published vision for Australia's A2A payments system: “a trusted account-to-account payments system that meets the evolving needs of consumers, businesses, and government agencies, supporting resilience, competition, innovation, and productivity in the Australian economy.”¹³ Action to achieve this vision should ensure that consumers and merchants can choose between cards, A2A, or other payment methods, with a clear understanding of the protections, costs, and operational implications of each.

This choice is not straightforward: card payments are secured by multi-layered fraud controls, network-level risk management, and enforceable chargeback rights. As the RBA itself notes, A2A models may involve different approaches to fraud, chargebacks, and liability allocation compared with card payments.¹⁴ Informed consumer choice, underpinned by consistent minimum protections, is the right policy objective.

Visa's specific responses to the questions raised in the Issues Paper are set out below.

¹³ A2A Payments Roundtable (2026), [Vision for Australia's A2A payments system](#), p3.

¹⁴ Reserve Bank of Australia (2026), [Review of Payments System Regulation Issues Paper](#), p14.

Issues for Consultation

Merchant Choice in Payments

Competition across debit card networks

Q1: What are the impediments to competition between debit card networks for merchants' transactions on dual-network debit cards (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?

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?

Visa supports preserving the RBA's approach to date on Least Cost Routing (LCR), in this case for online and mobile channels. This allows merchants to consider factors, such as authorisation rates, platform technology, security, value-added services, data and analytics capabilities, system resilience, innovation, and convenience, when making routing decisions. Experience with card-present (CP) LCR validates the market-led approach as the right model for extending LCR to online and mobile channels. As the RBA notes in the Issues Paper, as of December 2025, LCR for in-person transactions is available to 100 per cent of merchants and enabled for 84 per cent of them.¹⁵ Furthermore, the RBA's recent Review of Merchant Card Payment Costs and Surcharging Conclusions Paper found that "there is not a strong case for a formal regulatory requirement to enable LCR in the in-person environment," adding that the expectations-based approach best balances the benefits of LCR against the costs of implementation.¹⁶

The expectations-based approach continues to be most effective, given that the Australian debit card segment is characterised by effective and growing competition, including in mobile and online environments, and merchants continue to have genuine choice over how they route debit transactions. Competition for payments in this segment operates not only between Dual Network Debit Card (DNDC) networks but across a broader ecosystem that includes direct debit, BPAY, the New Payments Platform (NPP) and PayTo, Buy Now Pay Later (BNPL), and a range of emerging digital payment methods. The entry of digital-only acquirers has enhanced competitive dynamics within the payments ecosystem and expanded merchant access to alternative acceptance channels beyond conventional point-of-sale (POS) infrastructure.

The RBA's 2025 Consumer Payments Survey reflects the depth and dynamism of this segment: debit cards continue to account for approximately one in every two consumer payments, and account-to-account payment methods have grown substantially – with PayID usage rising by 18 percentage points between 2022 to 2025, to around 50 per cent of survey respondents in 2025. In addition, there has been growth in online payments, which now account for one in five

¹⁵ Ibid., p7.

¹⁶ Reserve Bank of Australia (2026), [Review of Merchant Card Payment Costs and Surcharging Conclusions Paper](#), p92.

consumer transactions. This has been driven in part by increasing use of PayPal and BNPL services alongside card payments.¹⁷

Against this backdrop, and as the RBA notes, competitive forces are already driving down weighted-average domestic debit interchange rates,¹⁸ demonstrating that the segment is functioning as intended and delivering outcomes aligned with the RBA's policy objectives. Specifically, the weighted-average interchange fee on domestic debit and prepaid card transactions has fallen to around 6 cents – below the benchmark of 8 cents per transaction and significantly below the new RBA caps of 8 cents or 0.16 per cent of transaction value.¹⁹ Furthermore, the current LCR environment has led networks to set strategic merchant rates across both large and small merchants to provide optimised economics to drive economic growth. This includes Visa's Acquirer Small- to Medium-sized Business (SMB) Program, which offers preferential interchange rates for domestic debit transactions to acquirers who support SMB growth on the Visa network.

Merchants continue to exercise routing choice on the basis of price and service, and ongoing investment in new capabilities, reflecting continued competitive discipline and commercial incentives to improve merchant outcomes. Every network a merchant supports is equally free to develop and deliver their product and innovation roadmap and offer the capabilities that earn that choice. Furthermore, the standards underpinning emerging commerce are open, not proprietary. Click to Pay, for example, is built on EMVCo's Secure Remote Commerce specifications²⁰, which any network can build to, allowing its participating merchants and acquirers to process transactions over its infrastructure. The same open-standards logic runs through e-commerce, tokenisation, digital wallets, and agentic commerce. Being considered by a merchant for a given use case or experience rests on each network providing value to the merchant's business, which is precisely the competitive discipline the RBA is seeking to promote.²¹

In addition, in certain cases, the provision of online debit-network choice sits above the network and acquirer layers. Specifically, integrated platforms or service providers can choose to route dual-network debit transactions to a single default network as part of a bundled offering. In such instances, a merchant's choice encompasses a broader value proposition beyond simply network choice.

Visa acknowledges that online and mobile LCR enablement is at an earlier stage than CP LCR. However, this reflects the complexity of coordinating multi-party integration across a layered online payment stack (acquirers, payment service providers (PSPs), gateways, and platforms), rather than a structural restriction on competition. This is consistent with the RBA's own analysis,

¹⁷ Reserve Bank of Australia (2026), [Consumer Payment Behaviour in Australia, RBA Bulletin, May 2026](#).

¹⁸ Reserve Bank of Australia (2025), [Review of Merchant Card Payment Costs and Surcharging Consultation Paper](#), p27.

¹⁹ Ibid.

²⁰ EMVCo (2026), [EMV® Secure Remote Commerce](#).

²¹ The RBA recognises the need to "balance the benefits of competition – such as lower costs and improved outcomes for end users – against the implementation costs and potential effects on efficiency and innovation in the payments system". Reserve Bank of Australia (2026), [Review of Payments System Regulation Issues Paper](#), p9.

which attributes the online gap to sequencing and integration economics – for example, eftpos enabling online functionality later than the international networks²², rather than due to any network foreclosing a competitor. Visa is itself actively enabling dual-network token provisioning and online LCR for its acquiring clients.

As the payments ecosystem enters the next stage of commerce and innovative technologies, the current approach – without further regulatory action on LCR – continues to achieve strong outcomes in supporting competition and innovation and helps avoid unintended consequences that could negatively impact safety and efficiency in the payments ecosystem. The RBA states that emerging payment use cases, such as agentic commerce, may exacerbate “existing constraints on competition between debit networks for online payment.”²³ However, as outlined above, in Visa’s experience, the standards underpinning emerging commerce are open for each network to invest in, and offer, the latest innovative and secure capabilities to merchants and acquirers. With the advent of new payment technologies and the need for ever-evolving approaches to help protect against fraud and scams, such continued innovation is critical to ensure merchants have access to the next generation of payments infrastructure and technology, especially in areas such as digital authentication, fraud protection, and security.

Tokenisation of card information

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?

Visa supports industry participants adopting token portability, synchronisation, and visibility based on their role in the ecosystem. These capabilities are available through Visa’s network tokenisation program and support a robust, competitive ecosystem. Specifically, token portability, as defined by the RBA in May 2024²⁴, allows merchants to port stored credentials between service providers; token synchronisation permits issuers to update PAN changes across held tokens; and token visibility enables cardholders to see which merchants have stored tokens. Visa has implemented these capabilities in Australia in line with the RBA’s May 2024 tokenisation expectations²⁵, which have functioned effectively in promoting adoption and raising security standards without prescriptive mandates.

In Visa’s assessment, this is itself clear evidence regarding the question of effectiveness: an expectations-based approach, rather than detailed regulation, has driven both adoption and a measurable uplift in security. Consistent with the position that Visa has previously set out on

²² Ibid., p8.

²³ Ibid.

²⁴ Reserve Bank of Australia (2024), [Expectations for Tokenisation of Payment Cards and Storage of PANs](#).

²⁵ Reserve Bank of Australia (2026), [Review of Payments System Regulation Issues Paper](#), p10.

debit-network competition²⁶, the standards that underpin tokenisation are open, and the onus on delivering portable, synchronised, and visible tokens rests with each network and provider competing for merchant and issuer relationships. Visa continues to invest in these capabilities on that basis.

Visa acknowledges the portability frictions the RBA describes when a merchant changes PSP.²⁷ However, it is important to recognise that the merchant and device binding of network tokens is a deliberate security feature, not a defect: restricting a token to a specific merchant or device is precisely what limits the damage if that token were to be compromised. The right approach to portability is, therefore, a well-defined network-level token-handover mechanism between service providers that preserves this binding, rather than de-binding tokens in a way that would reduce their security value. Visa's network tokenisation program supports porting stored credentials between providers while preserving these protections, and this can build on the same infrastructure as AusPayNet's data-porting standard (with which the RBA expected compliance by 1 July 2026).²⁸

On regulating token portability, Visa cautions against mandates that could undermine the competitive incentives to invest in tokenisation infrastructure. Any such requirement should only be considered where there is clear evidence of consumer harm arising from specific competitive impediments and should not inadvertently reduce security or shift liability in ways that disadvantage issuers and networks that have invested in tokenisation.

Looking ahead, Visa is designing its portability and synchronisation capabilities to be forward-compatible with the next generation of commerce, so that the same tokenisation infrastructure serves recurring payments, digital authentication and passkeys, and emerging agentic commerce. Preserving an expectations-based approach, and resolving concrete synchronisation collaboratively, positions Australia to realise the full security and fraud-reduction benefits of tokenisation without dampening the investment that has delivered progress to date.

Use of AI agents for payments in e-commerce

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 – the use of AI agents to discover, compare, and complete purchases on behalf of consumers – is a major opportunity for Australia's payments ecosystem and for the country's consumers and merchants. Research conducted by Visa finds that 73 per cent of shoppers across Australia, New Zealand, and the United States are interested in using AI agents

²⁶ Visa (2023), [Visa's submission to the Reserve Bank of Australia on the Australian Debit Card Market: Default Settings and Tokenisation](#).

²⁷ Reserve Bank of Australia (2026), [Review of Payments System Regulation Issues Paper](#), p10.

²⁸ Ibid., p11.

for discovery and exploration.²⁹ For merchants, agentic commerce can reduce friction-driven cart abandonment, lower customer acquisition costs, and improve conversion rates.

Visa's approach to agentic commerce

Visa's role in the agentic commerce ecosystem is not to operate the AI system itself, but to provide a trusted payments layer that ensures agent-initiated transactions can be conducted securely, transparently, and reliably. Our approach is, therefore, focused on enabling innovation while preserving trust, consumer consent, accountability, security, and interoperability across the ecosystem.

Visa recognises the competition and efficiency concerns identified by the RBA, including the importance of preserving merchant choice, transparency, and affordability as new agentic commerce models develop.³⁰ We set out below our perspectives on these matters as they relate to regulation. Visa supports competitive, interoperable, and open approaches that allow different ecosystem participants – including merchants, acquirers, issuers, payment networks, wallets, and technology providers – to participate on fair and transparent terms. At the same time, given the early stage of development, Visa cautions against prescriptive regulation that could prematurely constrain emerging models before technical standards, liability frameworks, and commercial practices have had sufficient time to mature.

We support a risk-oriented, outcomes-focused approach to the governance of emerging AI ecosystems, recognising the need to balance innovation with robust safeguards. Visa shares the Government's commitment for AI policy to provide flexibility to keep pace with change, while providing the certainty to support growth and investment.³¹ Any potential regulatory framework should be grounded in existing laws on payments and financial services, and take a proportionate approach to any AI-specific risks not covered by existing sectoral regulation. The core principles of any regulatory framework that the RBA might consider should include guidance to maintain clear authorisation criteria for agents engaged in performing high-risk, high-value, or sensitive functions, such that agent autonomy remains appropriately bounded by pre-established rules and controls.

Finally, Visa supports the approach that the Government has set out, in which any new AI policy initiatives should complement and be consistent with existing laws and frameworks while aiming to close specific, clearly identified gaps.³²

Disputes, liability, and fraud

²⁹ Visa (2026), [What happens when AI becomes the shopper?](#) Australia leads in readiness: 44 per cent of Australian consumers report they would be more likely to shop with a retailer that offers an AI agent, compared with 34 per cent in New Zealand – driven principally by the benefit of time savings.

³⁰ Reserve Bank of Australia (2026), [Review of Payments System Regulation Issues Paper](#), p11-12.

³¹ Prime Minister of Australia (2026), [AI in Australia's interests](#).

³² Australian Government (2025), [National AI Plan: Keep Australians safe](#). The Plan notes: "The government's regulatory approach to AI will continue to build on Australia's robust existing legal and regulatory frameworks, ensuring that established laws remain the foundation for addressing and mitigating AI-related risks. These frameworks are actively enforced and continuously adapted to emerging risks."

Visa takes the risks of disputes, liability, and fraud seriously in any context and has made significant investments to address the RBA's concerns about disputes, liability, and new fraud vectors in the specific context of agentic commerce. The risks that the RBA has identified in the Issues Paper regarding uncertainty about consumer intent, mismatched expectations, and new categories of fraud³³ are inherent to any emerging commerce modality. Visa has spent decades building the infrastructure required to address and manage these risks at scale.

For agentic commerce specifically, we have developed Visa Intelligent Commerce, which brings together AI-ready payment credentials, tokenisation, advanced authentication, payment signals, consumer consent controls, and fraud risk management to enable agents to search, compare, and pay on behalf of consumers in a secure and transparent way.³⁴ Tokenisation replaces sensitive card details with unique digital identifiers so that credentials are never exposed at any step; merchants that have adopted Visa Token Service for their digital payments have reduced payment fraud rates by more than half.³⁵ Visa has also introduced the Trusted Agent Protocol, an ecosystem-led framework developed with Cloudflare, to help merchants securely identify authorised AI agents, verify agent intent, and distinguish legitimate commerce from malicious automation or rogue bots — preserving merchant visibility into the consumer payment experience while supporting agent-driven checkout processes.³⁶

These capabilities are undergoing continuing robust testing to prepare for the next era of agentic commerce based on the foundations of trust and security. In April 2026, Visa launched its Agentic Ready Program in Australia, making it among the first countries in the world to participate in the Program. The Program enables banks and fintechs to test agent-initiated payments in production-grade, multi-seller environments using the same trusted credentials, controls, and protections that underpin Visa's network today.³⁷ To date, nine Australian financial institutions have joined the program, namely ANZ, Bank of Melbourne, BankSA, Cuscal, ING, Latitude Financial, NAB, St George, and Zip, using Visa's trust layer of tokens, identity, risk management, and consumer controls to test cross-platform agentic payments at scale.³⁸

Through such programs and solutions, including via collaboration with Australia-based clients, Visa remains deeply committed to serving as a key enabler of trust in the agentic commerce ecosystem and enhancing customer and merchant experience in e-commerce without compromising trust and reliability.

Merchant choice and costs

The RBA states that “payments processing using AI agents may initially be limited to international card networks, and it is not yet clear how and when merchants may be given a choice of debit

³³ Reserve Bank of Australia (2026), [Review of Payments System Regulation Issues Paper](#), p12.

³⁴ Visa (2025), [Visa Expands Visa Intelligent Commerce Across Asia Pacific](#).

³⁵ Visa (2026), [What happens when AI becomes the shopper?](#)

³⁶ Visa (2025), [Visa Expands Visa Intelligent Commerce Across Asia Pacific](#).

³⁷ Visa (2026), [Visa Welcomes Partners into Agentic Ready Program to Unlock Agentic Commerce](#).

³⁸ Ibid.

networks for processing debit payments”³⁹ within agentic commerce. As with earlier phases of e-commerce, every network is free to invest in the technical, security, and commercial capabilities required to support emerging agentic commerce use cases. Visa’s agentic commerce capabilities, including the Trusted Agent Protocol⁴⁰, are designed around open architecture and ecosystem participation, enabling merchants, acquirers, issuers, technology providers, and payment networks to interoperate on transparent terms.

As agentic commerce develops, merchants will be able to assess the commercial terms, benefits, and costs of the solutions available to them and determine whether participation aligns with their business objectives. Prescriptive regulatory requirements at this early stage could risk impeding development of more efficient future configurations and reduce the incentive to invest in agentic payment capabilities, even as global momentum accelerates.⁴¹

The RBA also expressed concern that fees associated with agentic commerce can “add to the cost of accepting payments for merchants.”⁴² From Visa’s perspective, any additional fee associated with agentic commerce should be assessed against the material value it can enable. In that regard, the RBA observes that these services “may offer convenience and automation benefits for consumers.”⁴³ For merchants, their adoption of agentic commerce will be driven by a commercial assessment of net benefit — whether the incremental revenue reached through agentic channels exceeds the incremental cost of acceptance. Where that calculus does not favour adoption, merchants will not participate. This voluntary, market-driven dynamic provides a natural and effective check on the cost concerns the RBA raises.

³⁹ Reserve Bank of Australia, [Review of Payments System Regulation - Issues Paper](#), p11.

⁴⁰ Github (2026), [visa/trusted-agent-protocol](#).

⁴¹ McKinsey & Company (2025), [The agentic commerce opportunity: How AI agents are ushering in a new era for consumers and merchants](#).

⁴² Reserve Bank of Australia (2026), [Review of Payments System Regulation Issues Paper](#), p11.

⁴³ Ibid.

Mobile Payments, Non-designated Card Networks and Buy Now Pay Later

Non-designated card networks

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

The Review presents an important opportunity to address the longstanding regulatory asymmetry between designated four- and three-party networks, particularly American Express. Since the early 2000s, the RBA has recognised that three-party networks compete directly with four-party networks for merchant acceptance, while reserving the right to reassess their treatment as market dynamics evolved.⁴⁴ Those dynamics have now materially changed.

The Payments System Modernisation Act has clarified that three-party and closed-loop networks fall within the regulatory perimeter of the PSRA. This reflects Parliament's clear intent that the RBA has the authority to regulate a broader range of participants and payment networks where necessary to promote competition, efficiency, and financial safety.⁴⁵ The question is, therefore, no longer whether the RBA has the power to act, but whether continued regulatory asymmetry remains consistent with the public interest.

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?

Visa shares the RBA's view that strong contestability is key to a well-functioning payments ecosystem.⁴⁶ As a result, payment networks that compete and perform substantially similar functions should be subject to comparable regulatory expectations where this is necessary to promote competition, efficiency, and financial safety.

⁴⁴ Reserve Bank of Australia (2005), [Payments System Board Annual Report – 2005 | Credit and Charge Cards](#); Reserve Bank of Australia (2001), [Designation of Credit Card Schemes in Australia](#).

⁴⁵ Parliament of Australia (2025), [Treasury Laws Amendment \(Payments System Modernisation\) Bill 2025 Second Reading](#).

⁴⁶ Reserve Bank of Australia (2025), [Review of Merchant Card Payment Costs and Surcharging Consultation Paper](#), p3.

Account-to-account Payments

Future of account-to-account payments

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

A2A payments are well-suited to the use cases they were designed for: payroll, superannuation, welfare, and account transfers. The NPP has improved speed and data capability, and the Bulk Electronic Clearing System (BECS) remains effective, particularly for bulk files. However, certain challenges may arise as A2A payments are extended into retail, online, in-app, and in-person commerce, where speed and low cost are necessary but not sufficient.

Efficiency in payments should be measured across the full transaction lifecycle, not just the cost of initiating a payment. A payment method that processes instantly but cannot handle fraud, scams, refunds, disputes, or failed payments efficiently imposes real costs on consumers, merchants, and participants, and erodes trust. Those costs are less visible but no less material.

The collapse of Bonza Airlines in April 2024 illustrates the stakes.⁴⁷ Customers who had purchased flights via PayTo/PayID, without the protections attached to comparable card transactions, had no chargeback rights when the airline entered voluntary administration. Thousands of consumers were required to pursue recovery through the administration process, with no intermediary on which to fall back. Comparably, Visa cardholders were able to secure refunds. This is the consequence of extending A2A into commerce before the consumer protections those environments require are in place.

The specific gaps in A2A that limit efficiency, competition, and financial safety are well-defined: no mandatory framework for authorisation and consent; no consistent payee validation; no standard dispute or refund process; no clear liability allocation between participants; inconsistent fraud and scam controls; and limited payment status transparency. These are structural weaknesses that become more consequential as A2A expands into new commerce contexts.

Access and competition challenges compound these gaps. Direct access to A2A infrastructure remains concentrated, onboarding processes are lengthy and costly, and indirect access models do not meet the needs of all providers. These barriers limit the diversity of participants that can build on A2A rails and reduce the competitive pressure that might otherwise drive improvement.

⁴⁷ Bonza Aviation Pty Ltd entered voluntary administration on 30 April 2024. See: Capital Brief (2024), [Bonza customers who used real-time payments network risk missing out on refunds](#). See also: CHOICE (2024), [Bonza airline collapse: Will customers get their money back?](#).

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?

Visa supports the RBA establishing clear, principles-based baseline expectations for A2A payments operating in retail and digital commerce. These should cover: authorisation and consent standards; payee validation and misdirection prevention; fraud and scam prevention obligations with clear participant responsibilities; dispute and refund processes with defined timelines and liability allocation; payment status transparency; and operational resilience requirements. Visa does not recommend that the RBA prescribe a specific technology, product model, or payment infrastructure. The objective should be outcomes for end-users, not uniformity of implementation.

Standardisation within the A2A ecosystem is a priority area. Fragmented approaches to payment status messages, reason codes, refund processes, dispute resolution, and fraud information sharing create inconsistent consumer experiences and reduce systemic trust. Standardisation should reduce unnecessary complexity and improve provider switching, while allowing participants to differentiate through better security, fraud prevention, and customer experience.

Visa also encourages the RBA to treat commercial sustainability as a clear design constraint. A2A infrastructure that requires participants to bear the full cost of fraud prevention, dispute handling, resilience, and customer support without a viable commercial model will not attract the investment needed to deliver safe, reliable services at scale.

Competition between cards and account-to-account payments

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?

The barriers to A2A payments in in-person and online commerce are not primarily technical. A digital wallet can help reduce front-end friction, but it does not resolve the underlying protection gaps that determine whether A2A is appropriate for consumer commerce. Front-end seamlessness and back-end safety are separate questions.

The Bonza collapse, referenced in Visa's response to Question 11, illustrates the risk.⁴⁸ In a checkout or wallet environment, consumers may not be prepared to readily identify which payment method carries chargeback rights, which provides a dispute process, and which leaves them with no practical recourse if a merchant fails. When different payment methods appear identical at the point of payment but carry materially different protections, the burden of understanding falls on consumers. This is not informed choice, and the risk scales with adoption.

⁴⁸ Ibid.

The same issue applies to merchants. A2A acceptance in retail environments requires more than payment initiation. It requires payment confirmation, with sufficient certainty for physical goods release, refund capability, exception handling, reconciliation, and integration into existing business systems. Seamless payment initiation is the straightforward part; the operational infrastructure required to run A2A in commerce reliably is not yet standardised.

As a result, Visa would not recommend that the RBA mandate accelerated A2A enablement through digital wallets ahead of establishing a commercially viable and enforceable consumer protection framework. The policy objective should be informed choice: consumers and merchants should be able to choose between payment methods, with a clear understanding of the protections, costs, and operational implications of each. Visa supports any RBA action being technology-neutral and focused on end-user outcomes, rather than engineering a particular infrastructure into a specific interface before the underlying protections are in place.

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

The RBA should be cautious about mandating broad interoperability across cards and A2A payments. Cards and A2A operate under materially different frameworks, and those differences are not legacy inefficiencies to be harmonised. They reflect deliberate design choices about who bears fraud risk, how disputes are resolved, what liability obligations attach to participants, settlement models, and the protections on which consumers can rely. Mandating convergence would require either lifting A2A to card-equivalent standards or diluting card protections to create artificial parity. The second outcome would reduce consumer safety for Australians, not improve it.

The stronger case for regulatory action is standardisation within the A2A ecosystem, where fragmentation creates real and avoidable harm. Priority areas include: authorisation and consent frameworks; payee validation and confirmation of payee standards; payment status notifications and reason codes; structured refund and dispute processes with defined timelines and liability allocation; fraud controls and information-sharing obligations; and operational resilience reporting.

Visa supports standardisation that strengthens safety, reliability, and consumer trust within the A2A ecosystem. We do not support regulation that requires materially different payment systems to adhere to a single operating model or runs the risk of eroding existing card consumer protections as a trade-off for interoperability.

Cryptography and Fraud Prevention

Cryptography in the payments system

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 its cryptographic practices through a combination of coordinated industry migration programs, adoption of stronger cryptographic standards, and preparation for future threats associated with quantum computing.

Industry initiatives

In this regard, a significant current initiative in Australia is the AusPayNet-led Advanced Encryption Standard (AES) Migration Program, which brings together networks, issuers, acquirers, and other ecosystem participants to coordinate the payments industry's transition from legacy Triple Data Encryption Standard (Triple DES) cryptography to AES-128 and AES-256. The program aims to support a consistent migration approach while maintaining interoperability across the payments system, and has increasingly focused on participant readiness, migration planning, dependencies, risks, and implementation progress.

While the migration from Triple DES to AES is an important near-term uplift, the payments industry is also preparing for a longer-term transition to post-quantum cryptography. Across the financial sector, organisations are undertaking cryptographic asset discovery, assessing reliance on quantum-vulnerable algorithms, building cryptographic agility, testing post-quantum cryptographic capabilities, and developing migration plans aligned to emerging international standards. These activities recognise that the transition to post-quantum cryptography (PQC) is expected to be a multi-year undertaking that will require careful coordination across technology providers, payment networks, financial institutions, and other ecosystem participants. Organisations must identify and manage cryptographic dependencies across networks, applications, devices, payment terminals, cloud services and third-party suppliers while maintaining security, interoperability and operational continuity. In Visa's experience, cryptographic resilience is no longer solely a cybersecurity issue; it is becoming a strategic technology transformation objective.

Visa-specific initiatives

Visa supports industry-led efforts, including the migration to AES, through its global cryptography program, providing migration guidance, phased implementation roadmaps for issuers and acquirers, and continued investment in stronger cryptographic controls across its network. We maintain cryptographic standards aligned to internationally recognised frameworks, including National Institute of Standards and Technology (NIST) standards and Federal Information Processing Standards (FIPS)-approved controls. Furthermore, Visa is

progressively implementing stronger encryption standards, modern authentication protocols, tokenisation, modernising digital certificates, and continue leveraging Hardware Security Module (HSM)-based key management across its products and services.

As part of its broader cryptographic resilience strategy, Visa launched a PQC Readiness Program in 2025 and is executing a multi-year roadmap that includes cryptographic asset discovery, quantum risk assessments, TLS 1.3 modernisation, pilot testing of post-quantum capabilities, and migration planning. Visa communicated these key cryptographic modernisation milestones and post-quantum preparedness expectations to clients and partners, encouraging them to align their own modernisation roadmaps with the milestones Visa has identified. Visa has also incorporated NIST-standardised post-quantum cryptographic algorithms, including Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) and Module-Lattice-Based Digital Signature Algorithm (ML-DSA), into its cryptographic standards framework, as appropriate. These activities are designed to build cryptographic agility, support future migration to quantum-resistant algorithms, and maintain operational continuity throughout the transition.

Assessment of effectiveness

These initiatives are well-positioned to support effective outcomes because they are industry-led, internationally aligned and focused on maintaining interoperability across the global payments ecosystem. International standards bodies, including NIST, EMVCo, PCI SSC, ISO and ANSI X9, are developing the technical foundations for the industry's transition to stronger cryptographic standards and, ultimately, post-quantum cryptography. AusPayNet's AES Migration Program will benefit from continued alignment with these international standards and evolving global migration approaches to minimise fragmentation and preserve interoperability across cross-border payment systems.

While significant work remains, Visa's assessment is that the payments industry's current trajectory is appropriate and reflects an increasing focus on addressing evolving cyber security and cryptographic risks. The industry's challenge is no longer identifying which cryptographic standards should be adopted, but executing a coordinated, multi-year transition across a highly interconnected ecosystem. Executing this transition will require significant and sustained investment across the payments ecosystem, reflecting the complexity of modernising legacy cryptographic infrastructure while maintaining security, interoperability, and operational resilience. The effectiveness of the initiatives outlined above will, therefore, depend on continued executive prioritisation and ongoing collaboration across industry participants, technology providers, and standards bodies.

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

Participants face a range of challenges in uplifting cryptography and broader cyber security practices across the payments ecosystem. While awareness of cyber threats and the need for stronger cryptographic standards is generally well established, implementing change across highly interconnected technology environments remains complex. Payment systems work with

a wide range of participants, technology providers, and service providers. As a result, changes to cryptographic standards often require coordinated implementation across multiple organisations to maintain interoperability and minimise disruption. Cryptographic migration timelines can, therefore, be influenced by broader ecosystem readiness, third-party dependencies, and technology refresh cycles. For example, the changing landscape includes Harvest Now, Decrypt Later (HNDL) risk related to post-quantum cryptography, where attackers can collect encrypted traffic today and simply store it. Once sufficiently powerful quantum computers are available, that data could potentially be decrypted if protected by vulnerable public-key cryptography.

A further challenge is that organisations must identify and modernise cryptographic dependencies across networks, applications, devices, payment terminals, cloud environments, and third-party systems, many of which have evolved over decades. As the industry prepares for post-quantum cryptography, participants are increasingly focused on cryptographic asset discovery, cryptographic agility, quantum risk assessments, and migration planning, while continuing to maintain operational continuity and resilience. The challenge extends beyond the replacement of individual algorithms, requiring comprehensive visibility into where cryptography is deployed, how it supports critical business processes, and how changes can be implemented without disrupting interconnected payment systems and services.

Additionally, legacy infrastructure remains a challenge for some participants, particularly where systems were not originally designed to support modern cryptographic standards. Addressing these challenges may require multi-year investment programs involving infrastructure replacement, application remediation, testing, vendor engagement, and specialised expertise. The scale and complexity of this transition can be significantly greater than that associated with many previous technology upgrades, resulting in substantial ongoing resourcing requirements and implementation costs across the payments ecosystem. Accordingly, the challenge is often less about identifying the required technical changes and more about coordinating and executing those changes in a secure, orderly, and interoperable manner across a broad range of participants.

More broadly, participants are managing an increasingly complex cyber security environment. Alongside cryptographic modernisation, organisations are investing in cyber resilience, fraud and scam prevention, operational resilience, cloud transformation, third-party risk management, and compliance with evolving regulatory requirements. In Australia, frameworks such as the Security of Critical Infrastructure (SOCI) Act have increased industry focus on cyber security governance, risk management, and resilience. Balancing these concurrent priorities can create challenges in securing the funding, specialist cyber security expertise, and executive attention necessary to deliver large-scale transformation programs while maintaining operational resilience and continuity.

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?

Visa considers that the RBA can play an important coordinating role in supporting industry-wide cryptographic uplift across the payments ecosystem. Given the interconnected nature of payment systems, successful migration depends on alignment across issuers, acquirers, processors, merchants, technology vendors and service providers. As noted in our response to Question 16, the primary challenge facing participants is often not a lack of awareness or technical standards, but the complexity of implementing large-scale change across interconnected environments while balancing competing cyber security, operational resilience, and technology investment priorities.

In this context, the RBA is well placed to facilitate coordination across the payments ecosystem and promote alignment among industry participants. By employing its system-wide perspective, the RBA can assist in identifying issues that may affect broader migration efforts while helping avoid duplication of existing standards-setting and industry-led activities.

The most effective way to achieve this would be through continued engagement with, and support for, existing domestic and international standards frameworks, including AusPayNet, NIST, EMVCo, PCI SSC, ISO and ANSI X9. These bodies already provide the technical expertise, governance structures and global interoperability required to develop, test and implement cryptographic changes consistently across the payments ecosystem. The RBA can complement these efforts by monitoring on emerging guidance and leading practices, including developments in other jurisdictions and guidance from organisations such as the UK National Cyber Security Centre (NCSC), which may help participants better understand emerging risks and implementation approaches being considered internationally.

The RBA can also help promote industry readiness by reinforcing the importance of early planning for future cryptographic transitions and encouraging participants to prioritise the assessment of cryptographic dependencies and migration challenges. By maintaining visibility of ecosystem-wide readiness, implementation risks and transition timelines, the RBA can help participants better understand potential barriers and support more effective planning for the broader migration to quantum-resistant cryptography.

Importantly, cryptographic uplift is best supported through alignment with internationally recognised standards and industry-led frameworks, rather than through the development of Australia-specific cryptographic standards or prescriptive domestic technology mandates. Given the global and rapidly evolving nature of cryptographic threats, payment systems are best protected through internationally recognised standards that support global interoperability and consistent security outcomes. An outcomes-based approach focused on resilience, risk reduction and alignment with internationally recognised standards will deliver more sustainable security outcomes than prescriptive technical requirements that may duplicate existing industry initiatives, increase implementation complexity, or become outdated as technology evolves.

Card payments fraud overseas

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?

Overseas CNP fraud remains an important financial safety issue for the Australian payments ecosystem, particularly given the cross-border nature of the risk and the more fragmented control environment that applies to overseas merchants, acquirers, and service providers. However, any assessment of whether additional regulatory intervention is required should be guided by current fraud outcomes and the effectiveness of existing controls.

Visa's data demonstrates a sustained improvement in fraud outcomes in Australia. Between 2020 and 2025, overall Visa card fraud rates in Australia fell by about 28 per cent, while both domestic and cross-border CNP fraud rates declined by approximately 40 per cent, reaching their lowest levels in the past six years.⁴⁹ These outcomes suggest that existing industry investment and layered fraud controls are delivering measurable improvements across the payments ecosystem.

Importantly, these improvements have been achieved despite an increasingly complex and evolving threat environment. Fraudsters continue to adapt their tactics, exploit new attack vectors, and leverage emerging technologies. Over the last five years, Visa has invested more than A\$18 billion (US\$13 billion) in technology and infrastructure to safeguard the integrity of the payments ecosystem and accelerate the decline in fraud rates.⁵⁰ Visa is continuously monitoring the dark web and working with third-party partners to understand how the landscape is evolving, while continuously analysing data and refining detections and mitigations to keep in lockstep with evolving threats.⁵¹ These efforts underscore that maintaining and improving fraud outcomes requires sustained investment in technology, security, fraud prevention capabilities, and ecosystem-wide controls.

Visa's fraud data for Australian-issued cards also demonstrates a sustained, measurable, and accelerating reduction in CNP fraud since 2023. Critically, both domestic and cross-border channels improved simultaneously across two consecutive years, a pattern that reflects systemic, network-wide control effectiveness rather than channel-specific or temporary improvements.

Cross-border CNP transactions carry a structurally higher fraud rate than domestic transactions, reflecting greater exposure to CNP activity, more fragmented control environments, multi-jurisdictional complexity, and the limited practical reach of domestic mitigation frameworks.

While AusPayNet's fraud statistics provide valuable insights into industry-wide fraud trends, Visa encourages the RBA to consider these data alongside other sources when informing policy

⁴⁹ Visa Fraud Reporting.

⁵⁰ Visa (2026), [Visa to Acquire BioCatch](#).

⁵¹ Visa (2026), [The evolution of payment fraud and how to stay ahead of the evolving threats landscape](#).

development. As the published statistics are based on a subset of participating networks and reflect calendar year 2024 outcomes, the RBA may also benefit from reviewing additional data sources that reflect different network coverage or reporting periods.

Taken together, these insights highlight the importance of considering a broad range of evidence when assessing fraud trends and potential policy responses. This points to the value of an evidence-based approach that takes into account both industry-wide indicators and the demonstrated effectiveness of existing mitigation measures to ensure any regulatory action that may be considered would be proportionate, targeted, and aligned to current risk conditions.

Visa's data suggests that targeted investments in authentication, tokenisation, machine learning-based fraud detection, and ecosystem accountability frameworks are delivering measurable improvements in fraud outcomes. The sustained improvement in Visa's CNP fraud rates in Australia is not attributable to any single control, but rather to the compound effect of a layered, technology-led security strategy aligned with the Visa Security Roadmap for Australia 2025-2028⁵². The roadmap is centred on continued investment in secure technologies, a data-driven and risk-based approach to fraud management, and strengthened ecosystem resilience against both fraud and scams.

Central to this strategy is Visa's sustained investment in authentication and tokenisation. We saw a fourfold increase in authenticated transaction volumes over the past three years. This reflects the adoption of stronger authentication methods, including biometric and in-app authentication, which are less susceptible to social engineering than traditional SMS one-time passwords. Separately, Visa Token Service (VTS) deployment across the Asia Pacific region has delivered a 58 per cent⁵³ fraud rate reduction on tokenised versus non-tokenised transactions.

Visa has also invested heavily in network-level fraud detection and ecosystem controls. Visa Advanced Authorisation applies machine learning across Visa's global network to support real-time fraud detection and helped Australian financial institutions prevent A\$722 million in fraud in a single year⁵⁴. Beyond issuer-level controls, programmes such as the Visa Integrity Risk Program (VIRP) and Visa Acquirer Monitoring Program (VAMP) focus on reducing fraud exposure at the merchant and acquirer level by increasing accountability across higher-risk merchant categories and digital commerce environments. These initiatives are particularly relevant in the cross-border context because they target fraud risks at their source, regardless of where the merchant is located.

Visa's experience suggests that targeted, ecosystem-level controls can be highly effective in reducing cross-border CNP fraud. Similar trends have been observed across other jurisdictions, including Singapore and the United Kingdom, suggesting that controls directed at merchant and acquirer risk management can achieve meaningful reductions in fraud exposure across the payments ecosystem.

⁵² Visa (2025), [Visa Security Roadmap for Australia](#).

⁵³ Visa (2024), [The transformative impact of tokenisation on commerce in Asia Pacific](#).

⁵⁴ Visa, 12 months ending June 2025, VisaNet (July 2024 to June 2025).

While Visa supports Strong Customer Authentication (SCA) as an important component of a layered fraud control framework, we do not recommend a regulatory mandate requiring issuers to apply SCA to overseas CNP transactions. The effectiveness of such a mandate would be inherently limited because the decision to invoke 3DS authentication sits with the merchant and its acquiring bank, rather than the issuer. Where an overseas merchant elects not to initiate authentication, the issuer has no operational ability to apply SCA to the transaction. As a result, an issuer-side mandate would not address the portion of residual overseas CNP fraud occurring on unauthenticated transactions and would have limited reach over overseas merchants operating outside Australian jurisdiction.

More broadly, any assessment of where regulatory effort will generate the greatest reduction in consumer harm should consider the relative scale of fraud and scams. Visa notes that scam losses in Australia are materially higher than CNP fraud losses and continue to increase, while card fraud rates are declining (Figure 1). Importantly, scams are fundamentally different from card fraud because the consumer is deceived into authorising the payment themselves. As a result, measures such as SCA, while highly effective in reducing unauthorised fraud, are not designed to address the underlying social engineering that drives scam losses.

Figure 1: Card-Not-Present Fraud vs Scam Losses: Australia

YEAR	CNP FRAUD – AUSPAYNET (ALL SCHEMES)	SCAM LOSSES – SCAMWATCH / ACCC	SCAMS AS MULTIPLE OF CNP FRAUD
2024	A\$816M	A\$2.0B	2.5×
2025 (partial)	A\$854M	A\$2.2B	2.6×

Sources: AusPayNet Fraud Statistics; Scamwatch / ACCC Targeting Scams Report · AUD · Card fraud declining; scam losses increasing

In response to this challenge, Visa has invested significant resources in dedicated scam disruption capability through the Visa Scam Disruption Practice (VSD) – a globally operating capability that proactively identifies, investigates, and dismantles complex scam networks before they reach consumers. Operating across the full scam supply chain from criminal infrastructure to payment delivery, and drawing on Visa's proprietary transaction intelligence, AI-powered detection, and cross-sector partnerships with financial institutions and law enforcement, the VSD has identified over A\$3.7 billion (US\$2.6 billion)⁵⁵ in attempted scam-related fraud globally since its creation just over two years ago.

In addition, as scams continue to scale, prevention needs to be applied more systematically across the ecosystem. This is why VIRP has evolved to encompass a broader range of scams and security threats, including scams, transaction laundering, collusion, and other deceptive business practices. This expansion reflects the growing convergence of fraud, scams, and organised criminal activity within the global payments ecosystem. In Asia Pacific, this approach is complemented by the Merchant Elevated Risk Program (MERP) which was introduced in 2026 to

⁵⁵ Visa (2026), [Visa announces latest milestone for pioneering Scam Disruption Unit.](#)

focus on identifying merchants that show clear indicators of elevated risk, such as unusual transaction spikes, higher fraud or dispute ratios, or inconsistent activity patterns. This introduces an additional layer of protection and clearer reimbursement pathways for cardholders where appropriate.

Accordingly, any regulatory response that the RBA may consider should be targeted, evidence-based, and focused on the controls that can most effectively reduce consumer harm. The recent decline in fraud rates demonstrates the value of continued investment in authentication, tokenisation, machine learning-based fraud detection, acquirer accountability frameworks, and other network-level controls. These types of ecosystem-wide interventions are likely to deliver more sustainable outcomes than a broad issuer-side mandate that does not address the underlying drivers of residual overseas CNP fraud.

About Visa

Visa is a world leader in digital payments. Our mission is to connect the world through the most secure, reliable, and innovative payments network – enabling individuals, businesses, and economies to thrive. Our innovative technologies facilitate global commerce and money movement across more than 200 countries and territories and among consumers, financial institutions, businesses, strategic partners, and government entities.

Visa has operated in Australia since the early 1980s and currently has offices in Sydney and Melbourne. Together with our partners, we are committed to building a future of commerce that fosters Australia's economic growth, security, and innovation. Over a five-year period, Visa has invested more than A\$18 billion (US\$13 billion) in systems resilience, fraud management and cybersecurity, including tokenisation, AI, and blockchain-based solutions, to bring even more security to every transaction, helping protect consumers and businesses.⁵⁶ In the 12 months ending June 2025, Visa Advanced Authorisation (VAA), Visa's AI-based real-time payments fraud monitoring solution, helped Australian financial institutions to prevent A\$722 million in fraud from disrupting the nation's businesses.⁵⁷

Visa welcomes being able to make wider contributions to Australia to foster inclusive economies where individuals, businesses, and communities can thrive. In April 2026, Visa announced the eight recipients of the A\$200,000⁵⁸ Visa Vibe Grants Program, delivered in partnership with Mainstreet Australia,⁵⁹ recognising businesses and community organisations that are reimagining Australia's night-time economy. Through the Program, one recipient from each state and territory received A\$25,000 to activate public spaces after dark and create more affordable, safe, and inclusive community experiences.

In Australia, the Visa Foundation recently awarded Thread Together a A\$285,000 (US\$200,000) grant to expand its national service delivery model, helping redistribute surplus new clothing to people experiencing hardship, including women and children escaping family and domestic violence, as well as people living in regional and remote communities and those affected by natural disasters.⁶⁰

The Visa Foundation is also an investor in the First Australians Capital Catalytic Impact Fund, which supports Indigenous businesses and enterprises and helps advance greater economic independence. To date, the Foundation has committed A\$2 million to the Impact Fund. Prior to this, in 2023, the Visa Foundation provided funding to the Australian not-for-profit, Good Return, to support Indigenous women entrepreneurs in Australia.⁶¹

⁵⁶ Visa (2024), [Security Roadmap Australia 2025-2028](#).

⁵⁷ Visa, 12 months ending June 2025, VisaNet (July 2024 to June 2025).

⁵⁸ Visa (2026), [Visa Vibe Grants Program 2026](#).

⁵⁹ Mainstreet Australia (2026), [Mainstreet Australia](#).

⁶⁰ RagTrader (2026), [Thread Together secures US\\$200k grant](#).

⁶¹ Good Return (2023), [Good Return receives funding from Visa Foundation to support Indigenous women entrepreneurs in Australia](#).

Additionally, Visa invests in initiatives that promote inclusion and connect people, businesses, and communities through sport. Visa is the Official Global Supporter of the AFC Women's Asian Cup Australia 2026 and was a partner for FIFA World Cup Australia & New Zealand 2023. Through its "Let's Get On Her Side" campaign⁶², Visa encourages positive support, respect, and inclusion for women in sport. In addition, Visa sponsors the Australian Olympic Team, as well as Team Visa Olympians Scotty James, Flynn Southam, Ellie Carpenter, and Molly Picklum, and Paralympian Jaryd Clifford.

In 2025, Visa announced the opening of a new regional office in Suva, Fiji, which enhances our ability to support partners and clients in Fiji and other Pacific Islands, and reinforces our commitment to fueling innovation and accelerating the region's digital transformation. Visa has been working with several partners in the Pacific Islands, including not-for-profit Good Return, to promote the adoption of secure, convenient, and reliable payment solutions through financial education.⁶³

Visa is honoured to support Papua New Guinea's national rugby league team, the PNG Kumuls, as their first global sponsor. We also support two Pacific Islands rugby players as Visa Ambassadors: Jerry Tuwai, Fijian Olympic gold medalist, and Stanley Gene, Papua New Guinean rugby league legend. These partnerships reflect our commitment to Fiji and Papua New Guinea's development and sport's unifying power.

⁶² Visa (2026), [Visa rallies fans to back women beyond the win this AFC Women's Asian Cup with 'Let's Get On Her Side'](#).

⁶³ Visa (2025), [Visa launches office hub in Fiji, setting a new path for growth across the Pacific Islands](#).