29 August 2025

Dear Department of Home Affairs representative,

Visa's response to the Charting New Horizons - Developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy: Policy Discussion Paper

Visa welcomes the opportunity to contribute to the Australian Government's consultation on the Charting New Horizons – Developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy (the Strategy). We share the Government's ambition to make Australia a world leader in cyber security – a priority underscored by recent global incidents impacting supply chains, infrastructure, governments, and businesses of all sizes.

As a global leader in payments technology, Visa operates at the intersection of cyber security, operational resilience, and fraud prevention. Visa secures the payment ecosystem with a four-pronged approach:

1. **Protect against potential threats**: We champion industry-wide payment security standards, establish comprehensive solutions to secure the full transaction lifecycle and guide stakeholders to support the use of secure technologies and practices.
2. **Defend against ongoing attacks**: We monitor ecosystem participants for vulnerabilities, use actionable intelligence to detect and alert others against fraud and implement compliance programs to remediate fraud, disputes or illegal activity.
3. **Evolve capabilities in a shifting landscape**: We embed security into all channels and flows from day one of product and system development and share recommended best practices for ecosystem participants to benefit from network-level lessons learned.
4. **Tailor risk management to unique needs**: We offer a suite of capabilities for clients across the risk management value chain, including through our Risk-as-a-Service (RaaS) capabilities, delivered as self-service modules or as a managed service via our Risk Operations Centre.

This submission outlines how Visa can help advance the Strategy's objectives through industry collaboration, standards leadership, and scalable innovation - particularly in support of small and medium-sized businesses (SMBs), not-for-profits, and the broader digital economy.

Shield 1: Strong Businesses and Citizens

Visa strongly supports the focus on strengthening cyber resilience for SMBs, not-for-profits, and individual Australians. These groups are often disproportionately affected by cyber

threats due to limited resources and technical capacity, making targeted support essential. Expanding access to targeted education, practical tools, and advisory resources is critical to enabling them to manage cyber risks more effectively.

Recent findings from the Australian Institute of Criminology underscore the urgency of strengthening cyber resilience across the community. According to the Cybercrime in Australia: 2024 report, nearly half (47%) of Australian internet users experienced some form of cybercrime in the past year - including identity theft, scams, malware, and online abuse[1]. This figure highlights the importance of expanding access to cyber awareness, education, and practical tools - particularly for those with limited resources or technical capacity.

Visa's initiatives, including the **Payment Cybersecurity Institute** and certification programs delivered through **Visa University**, are designed to uplift cyber maturity across the payments ecosystem and can be employed more broadly to support the wider industry. As a founding member of the Payment Card Industry Security Standards Council (PCI SSC), Visa plays a leading role in developing and promoting global standards, such as the Payment Card Industry Data Security Standard (PCI DSS). These standards establish clear requirements and are designed to be adaptable to organisations of varying size and complexity, helping to establish foundational security practices across the ecosystem. Visa recognises that foundational cyber hygiene remains one of the most effective defences against evolving threats. Practices such as timely software updates, strong authentication credentials, and the use of phishing-resistant multi-factor authentication - like passkeys - can significantly reduce exposure to ransomware, scams, and other malicious activity. In parallel, continued investment in identity protection and post-incident support services is essential. Visa is proud to partner with initiatives such as the **Australian Signals Directorate's Cyber Security Partnership**, which helps build awareness and resilience across communities, including among small businesses and not-for-profits.

Visa maintains a deep and evolving understanding of threats across the payments ecosystem, including their impact on individuals and businesses. These insights are shared with the community through confidential and public Bi-Annual Threat Reports. For example, from July through December 2024, Visa Payment Ecosystem Risk and Control (PERC) identified global ransomware attacks and data breaches that were opportunistic in exfiltrating data, with several thousand incidents tracked - a 51 per cent increase compared [2] the prior six-month period. The prevalence of ransomware attacks and data breaches across sectors underscores a critical reality that threat actors will attempt to exploit any vulnerability they can find. This reinforces why ongoing investment in cybersecurity, strong cyber hygiene practices, and

[1] The Hon Tony Burke MP (18 August 2025), New national report reveals extent of cybercrime in Australia
[2] Visa (2025), Visa Biannual Threats Report

cross-sector collaboration are essential to defend the ecosystem. To address these threats, Visa PERC works closely with global law enforcement to disrupt fraud campaigns and disseminate actionable intelligence. Combined with Visa's broader community partnerships and educational initiatives, these efforts help equip businesses and individuals to strengthen their defences against both current and emerging cyber risks.

Shield 2: Safe Technology

Visa recommends embedding global best practices in secure payment technologies, data governance, and responsible use of emerging technologies, such as Artificial Intelligence (AI). Through our leadership roles in the Payment Card Industry Security Standards Council and EMVCo, we have advanced technology-neutral and outcome-based standards that keep pace with innovation while maintaining strong protections. Security by design should be a foundational principle for emerging technologies. We encourage adoption of frameworks that enable secure data sharing and promote innovation without compromising trust.

Shield 3: Threat Sharing and Blocking

A proactive, intelligence-driven cyber security posture is essential. Visa supports the expansion of existing platforms, such as the Trusted Information Sharing Network. Visa has also started piloting threat intelligence services for financial institutions through our Threat Intelligence Fusion Platform, originally built internally to synthesise and understand varied threat intelligence streams. We also advocate for implementing responsible vulnerability disclosure mechanisms, including for scam-related vulnerabilities, to accelerate remediation efforts while safeguarding all stakeholders.

Beyond engagement with individual governments, Visa knows first-hand the benefits of international collaboration in cyber security, leading to fast and frictionless information sharing across borders, for the benefit of all ecosystem participants and the customers they serve. Initiatives such as the European Cyber Resilience Board (ECRB) and the Financial Services Information Sharing and Analysis Center (FS-ISAC) in the United States involve multiple organisations working together through formal contractual arrangements and informal partnerships – across both the public and private sectors – to achieve greater global resilience to cyber attacks.

Visa recommends that Australia build on existing efforts, such as the Australian Signals Directorate's Australian Cyber Security Centre's (ACSC) Cyber Security Partnership Program and the Australian Government's Trusted Information Sharing Network, as well as deepen engagement with trusted intelligence-sharing communities and initiatives. Sharing reliable, contextualised technical intelligence – such as indicators of compromise – via a centralised

threat intelligence platform, with members contributing in near real-time, significantly benefits the broader ecosystem.

Shield 4: Protected Critical Infrastructure

Visa supports proportionate, risk-based regulatory frameworks that reflect the maturity and operational realities of each sector. Visa supports regulation being outcomes-focused, adaptable to evolving threats, and technology-neutral, avoiding prescriptive requirements that may quickly become outdated. We also encourage the use of sector-specific maturity assessments, supported by government-provided tools, guidance, and incentives to uplift resilience. Through our active participation in global standard-setting bodies, Visa contributes to secure, interoperable, and scalable frameworks that protect critical infrastructure while enabling innovation.

Shield 6: Global and Regional Leadership

Visa is committed to supporting Australia's leadership role in cyber security across the Asia-Pacific region. Regulatory harmonisation across jurisdictions will be important to reduce complexity and strengthen interoperability, while deeper engagement with Southeast Asia and the Pacific regions will help build a resilient regional cyber ecosystem. Visa welcomes the Australian Government's efforts to enhance cyber resilience and strengthen cyber incident preparedness and response across the region[3]. Australia is well positioned to share best practices and capacity-building initiatives, and Visa stands ready to partner in these efforts.

In August 2025, Visa launched its global Cybersecurity Advisory Practice, a dedicated initiative to help payments ecosystem stakeholders proactively assess and strengthen their defences against emerging threats. This practice draws on Visa's global expertise and includes services such as cybersecurity maturity assessments, threat intelligence, and employee training through the Payment Cybersecurity Institute. These investments are now being employed globally to support businesses in building cyber resilience and navigating complex regulatory environments across geographies[4].

Visa is committed to supporting the Government's vision for a cyber secure nation by 2030. We see a future where Australia leads globally in cyber resilience, with a digitally confident population, secure businesses of all sizes, and a thriving regional ecosystem built on trust and collaboration. With our global expertise, advanced security capabilities, and deep operational insights, we can play an active role in strengthening Australia's cyber resilience and ensuring its position as a world leader in the digital economy. We support the adoption of zero trust architecture, defence-in-depth models, and secure-by-design principles, alongside

[3] Australian Government, Department of Foreign Affairs and Trade, Shared security in the Pacific
[4] Visa (2025) Visa Extends Cybersecurity Expertise, Prioritising Proactive Defence Strategies for Clients

investments in AI-driven threat detection and supply chain risk management. These actions, combined with scalable innovation and public-private collaboration, will help Australia defend against evolving threats and build a resilient digital economy.

We welcome the opportunity to provide further detail on our recommendations and to participate in targeted discussions as the Strategy progresses.

Yours sincerely,