Securing Malaysia's Digital Payments Ecosystem in the AI Era

Visa Public

Table of Contents

Malaysia's payments revolution reshapes its threat landscape

Malaysia's digital economy grew faster than its GDP in 2024. ICT and eCommerce contributed 23.4%, or RM451.3 billion,[1] to Malaysia's economy in 2024, significantly outpacing GDP growth in the country. As the fastest growing digital economy in Southeast Asia, the country's digital economy was valued at roughly US$39 billion in 2025, growing at 19% year on year.[2] This growth is expected to continue.

However, as Malaysia's digital economy grows, fraud and scams have kept pace. According to the Home Ministry, Malaysians lost RM2.97 billion to scams in 2025, the highest annual figure in three years. In addition, card-not-present (CNP) fraud, the kind that thrives on remote, screen-based transactions, has become the largest source of fraud losses in the country.

Yet this is not a story of controls standing still. Banks successfully blocked approximately RM1.2 billion in fraudulent transactions in 2025[3], compared to RM399 million in 2024, reflecting stronger fraud controls and greater vigilance across the financial sector.

Nevertheless, reported fraud cases continued to rise as cybercriminals adopted increasingly sophisticated tactics, including malware capable of compromising customer devices and enabling unauthorised fund transfers.

Understanding how these threats are evolving is critical for organisations seeking to grow securely in an increasingly digital economy. This challenge sits at the heart of Visa's Malaysia Security Roadmap 2026-2028.

1. Department of Statistics Malaysia (DOSM), "Malaysia Digital Economy, 2025" (ICT & e-commerce contribution). https://www.dosm.gov.my/portal-main/release-content/malaysia-digital-economy-2025
2. e-Conomy SEA 2025 Malaysia report: Malaysia e-Conomy SEA 2025 report
3. BNM Financial Stability Review 2H 2025: BNM Financial Stability Review

The new face of fraud

The fraud landscape is undergoing a fundamental shift. Traditionally, fraudsters focused on compromising payment credentials, exploiting system vulnerabilities and stealing card data. Today, fraudsters are increasingly targeting people rather than technology, exploiting trust, urgency and human behaviour to deceive consumers into making payments themselves.

At the same time, cybercriminals are becoming more sophisticated. AI, automation and readily available cybercrime tools have lowered the barrier to entry, enabling attacks to be launched at greater speed, scale and precision. Deepfakes, synthetic identities and AI-generated content are creating new challenges for organisations seeking to authenticate users and protect digital identities.

These shifts are already visible in Malaysia. Visa data shows Malaysia's card-not-present fraud rate increased by 44% in 2025, while the Asia Pacific average declined by 15% over the same period. At the same time, scams such as investment scams, impersonation scams and shopping scams continue to gain prominence, reflecting a broader shift towards fraud that exploits trust and human behaviour rather than technical vulnerabilities alone.

Looking ahead, the rapid advancement of frontier AI models is reshaping both commerce and cybercrime. As AI agents, digital identities and automated decision-making become more prevalent, organisations will need to prepare for new forms of fraud, impersonation and identity abuse while continuing to deliver seamless digital experiences.

As fraud becomes increasingly interconnected and cross-border in nature, security can no longer rely on individual organisations acting alone. Stronger cybersecurity, modern authentication, secure payment credentials and greater ecosystem collaboration will be critical to sustaining trust in Malaysia's digital economy. These evolving threats form the foundation of Visa's Malaysia Security Roadmap 2026-2028.

In the AI era, the greatest vulnerability is no longer technology. It is human trust.

Building Trust in Malaysia's Digital Payments

The Security Roadmap 2026-2028

Malaysia's digital economy is growing rapidly, bringing convenience, innovation and inclusion, but also more sophisticated fraud and cyber threats. Visa's Malaysia Security Roadmap 2026–2028 sets out six priorities to strengthen trust, resilience and security across the payments ecosystem, preparing the industry for the next stage of digital growth.

Strengthening cybersecurity to anticipate emerging threats and enhance ecosystem resilience

Malaysia's rapidly growing digital economy is expanding both opportunity and risk. Data breaches, ransomware, supply chain attacks and third-party vulnerabilities are growing across sectors, making vendor oversight and incident response critical for organisations. Visa's roadmap stresses strong cybersecurity governance, PCI DSS compliance, proactive risk assessments and effective third-party risk management as crucial requirements. For issuers, acquirers, processors and service providers, resilience now means going beyond compliance and adopting a continuous approach to cyber risk management as strong cybersecurity controls are essential to protect consumer trust and sustain Malaysia's digital growth.

Advancing authentication for a seamless and secure digital experience

Fraudsters are increasingly exploiting phishing and social engineering to undo traditional authentication techniques, particularly SMS OTPs. While financial institutions have reduced their reliance on SMS OTP through the adoption of in-app authentication, the next evolution in digital identity lies in biometrics and passkeys. These technologies can deliver stronger security, improved protection against phishing and impersonation attacks, and a more seamless customer experience. In addition, richer authentication data also helps merchants and acquirers assess risk better and improves decision-making, thereby reducing fraud from compromised credentials while improving the customer experience.

Enabling safer transactions with tokenised payments

Protecting payment credentials is a growing priority as digital commerce expands, and tokenisation helps by replacing sensitive card data with unique digital tokens that are of no value to fraudsters. In Malaysia, this has already lowered fraud rates and lifted transaction approval performance. For instance, Visa Token CNP transactions in Malaysia delivered a 56% reduction in fraud compared with PAN-based CNP transactions in 2025, alongside a 4.5% lift in approval rates.[4] As adoption grows, tokenisation could help secure a safer, more innovative and seamless digital payments ecosystem for issuers, acquirers, merchants and fintechs. Furthermore, tokenisation is a foundational capability for payment innovations such as agentic commerce.

4. VisaNet, Jan-Dec 2024. Visa credit and debit card-not-present transactions for tokenized vs non-tokenized credentials in the AP region.

Transforming eCommerce checkout to enhance consumer confidence and convenience

The checkout experience is now as much about security as satisfaction, as complex flows, repeated credential entry and payment security worries all drive customer abandonment. Customers today are demanding safer and seamless payment experiences. Innovations such as Click to Pay, built on EMV® Secure Remote Commerce standards, help reduce checkout friction by minimising manual card entry and reducing exposure of sensitive payment credentials through tokenisation and secure authentication. Emerging solutions such as Visa Flexible Payment (Flex) further enhance the checkout experience by giving consumers greater control over how and when they pay. Together, these capabilities help deliver safer, more seamless and more personalised payment experiences, improving conversion rates for merchants while strengthening consumer confidence in digital commerce.

Leveraging foundational standards to drive network performance

With growing payment volumes, strong governance, fraud reporting and ecosystem accountability matter even more. Visa Malaysia has enhanced several ecosystem-wide programmes, including the Fraud Reporting and Control Program (FRECOP), Visa Acquirer Monitoring Program (VAMP), Visa Integrity Risk Program (VIRP) and Merchant Elevated Risk Program (MERP), to strengthen fraud visibility, improve risk management and reinforce accountability across the payments ecosystem. For issuers, acquirers and merchants, strong compliance and reporting standards help improve fraud management, network performance and trust.

Building a resilient payments ecosystem to combat fraud and scams in the AI era

Malaysia’s fraud landscape is quickly evolving as scammers use AI, automation and social engineering to increase investment scams, impersonation scams and account takeover attacks. AI, however, is also a part of the solution, with solutions like Visa Protect, which helps with AI-driven risk analytics, behavioural monitoring and real-time fraud detection that enables better fraud prevention outcomes. Visa Scam Disruption (VSD) – which leverages Visa's intelligence, analytics and cross-ecosystem visibility – also identifes, investigates and disrupts scam operations before they can scale. Globally, VSD has helped dismantle scam networks and supported efforts to prevent millions of dollars in potential fraud losses. Combined with stronger collaboration across regulators, financial institutions, merchants, payment providers and technology partners, these capabilities help build a more resilient payments ecosystem and strengthen protection for consumers in the AI era.

What this means for leadership

Malaysia's digital economy will continue to grow, but so will the sophistication of fraud, scams and cyber threats. As fraudsters increasingly target identities, trust and human behaviour, security can no longer be viewed solely as a compliance requirement. It has become a strategic enabler of growth, innovation and consumer confidence. In an increasingly digital economy, trust will be a key differentiator for organisations seeking to scale securely and sustainably.

Strengthen cyber resilience.

As organisations become more interconnected, cyber risk increasingly extends beyond internal systems to third-party providers, supply chains and digital ecosystems. Leaders should prioritise continuous cyber resilience, improve oversight of critical partners and ensure incident response capabilities can keep pace with a rapidly evolving threat landscape.

Modernise identity and authentication.

Accelerating the adoption of biometrics and passkeys can help reduce reliance on vulnerable methods such as SMS OTP, while delivering a more secure and seamless experience for legitimate users. As digital commerce expands and fraud tactics continue to evolve, stronger identity and authentication capabilities will become increasingly critical to balancing security, convenience and trust.

Strengthen ecosystem-wide resilience.

Fraud and scams are increasingly interconnected and cross-border in nature. Long-term success will depend on stronger collaboration, intelligence sharing and coordinated action across regulators, financial institutions, merchants, technology providers and consumers to collectively strengthen the resilience of Malaysia's payments ecosystem.

Call to action

Trust is Malaysia's next growth currency. As digital payments continue to evolve, securing the future of the ecosystem requires a shared commitment from every participant. No single organisation can combat fraud, scams and cyber threats alone. Success will depend on collective action to strengthen security, modernise authentication, protect consumers and build resilience across the ecosystem.

- For **regulators**, enable secure innovation through responsible AI, strong data protection frameworks and modern security standards.
- For **issuers**, accelerate the adoption of stronger authentication, AI-driven risk intelligence and secure payment experiences.
- For **acquirers and merchants**, strengthen onboarding, oversight and secure commerce capabilities that enhance both security and customer experience.
- For **third-party service providers**, maintain strong security controls and uphold the standards that underpin trust across the ecosystem.
- For **consumers**, remain vigilant, protect personal information and make use of available security controls and alerts.

One ecosystem. Shared responsibility. Together, we can build a safer, more trusted and more resilient digital payments ecosystem for Malaysia.

Only by securing payments and protecting every transaction can we safely power Malaysia's digital economic growth in the AI era.

For more information, please contact your Visa Risk Manager or visit visa.com/security