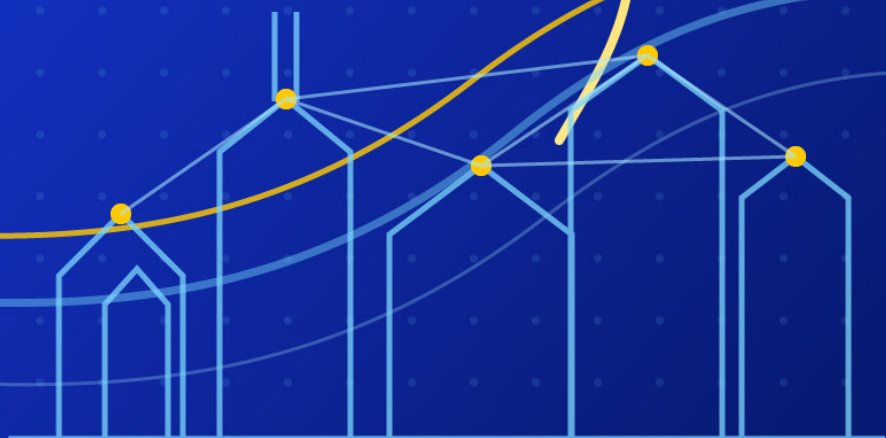
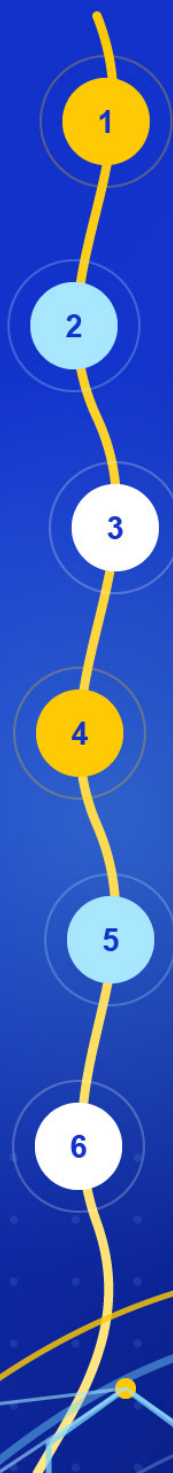




Singapore
2026 and Beyond

Security Roadmap

Visa Public



Contents

Executive summary	3
The journey	5
Lesson learnt	6
A changing world	7
Understanding the new threat landscape	8
Navigating Singapore's Evolving Fraud Landscape	9
National Drive Against Scam and Cyber Fraud Threats	10
Securing Singapore's Digital Payments Ecosystem in the AI Era: Visa Security Roadmap 2026 and Beyond	11
1. Strengthening cybersecurity to anticipate emerging threats & enhance ecosystem resilience	12
2. Advancing authentication for a seamless & secure digital experience	14
3. Enabling safer transactions with tokenised payments	15
4. Transforming eCommerce checkout to enhance consumer confidence & convenience	17
5. Leveraging foundational standards to drive network performance	19
6. Building a resilient payments ecosystem to combat fraud and scams in the AI era	23
Looking ahead	27
Call to action	28

As-Is Disclaimer

Case studies, comparisons, statistics, research and recommendations are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. Visa Inc. neither makes any warranty or representation as to the completeness or accuracy of the information within this document, nor assumes any liability or responsibility that may result from reliance on such information. The information contained herein is not intended as investment or legal advice, and readers are encouraged to seek the advice of a competent professional where such advice is required.



Executive summary

The payments ecosystem has changed more in the past 5 years than in the previous 50.



In a rapidly evolving technological landscape, businesses need to adapt quickly to grow sustainably. This shift isn't just about technology; it's about meeting the new expectations of digital-savvy consumers who seek personalised, convenient and secure experiences. Companies must be quick to respond to new trends and technologies, be it in data analytics or artificial intelligence (AI). This means making strategic investments and ensuring their workforce is skilled to make the most of these tools.

In Singapore, 56.4% of firms in the financial and insurance sector have adopted AI, among the highest adoption rates across industries.¹

While the democratisation of technology – and most recently AI – has benefited people and businesses, it has also emboldened bad actors. The incentive for criminal activity in the digital domain has never been easier and more enticing than it is today.

The consumerisation of cutting-edge technologies and the proliferation of new payment assets have also given rise to a new generation of cyber criminals, where hacking can now be a side hustle.

This has led to a clear evolution in the fraud and scam threat landscape. The increased sophistication of cyber attacks, powered by AI and automation, continues to drive traditional unauthorised fraud through more damaging and targeted data breaches. However, there is also a significant shift from this unauthorised activity towards authorised payment scams. Fraud is adapting from technical compromise to behavioural manipulation, exploiting trust and urgency to deceive consumers into making payments.

¹ Ministry of Manpower, "Inaugural Release of Report on Adoption of Artificial Intelligence Among Firms," 30 April 2026, <https://www.mom.gov.sg/newsroom/press-releases/2026/0430-adoption-of-ai-among-firms>

Executive summary continued

AI is also part of the solution. Visa has pioneered AI models in fraud protection since 1993, and today, our technology platform is among the most powerful examples of the tangible benefits of AI. Visa has over 150 AI and machine learning models in production, powering products that help to solve longstanding challenges and pain points for consumers, merchants and financial institutions.

The development and release of secure technologies, such as tokenisation and authentication, have established a new foundation for digital payments security. This latest Visa Security Roadmap looks at the biggest challenges facing the payments ecosystem in the coming few years and the steps we can take together to minimise the impact on consumers, merchants and other participants.

In this Roadmap we will look at:

- Strengthening cybersecurity to anticipate emerging threats & enhance ecosystem resilience
- Advancing authentication for a seamless & secure digital experience
- Enabling safer transactions with tokenised payments
- Transforming eCommerce checkout to enhance consumer confidence & convenience
- Leveraging foundational standards to drive network performance
- Building a resilient payments ecosystem to combat fraud and scams in the AI era

Visa is committed to connecting the world through the most innovative, convenient, reliable and secure payments network, protecting the payments ecosystem and facilitating global commerce for consumers, financial institutions, businesses, fintech partners and government entities.

Our network spans:



MORE THAN
200+
COUNTRIES AND TERRITORIES



APPROXIMATELY
~14.5K
FINANCIAL INSTITUTIONS



MORE THAN
175M+
MERCHANT LOCATIONS



~5B
PAYMENT CREDENTIALS



US\$17T
IN TOTAL VOLUME



329B
TOTAL TRANSACTIONS
in its fiscal year 2025²

² Visa Fact Sheet, Sep 2025, <https://corporate.visa.com/content/dam/VCOM/corporate/visa-perspectives/documents/about-visa-factsheet.pdf>

The journey

Since our first Visa Singapore Security Roadmaps in 2019 and the revised version in 2023, the payment landscape has transformed, bringing new conveniences but also a new generation of threats. The evolution from predictable fraud to sophisticated, AI-driven attacks and authorised payment scams demands a more dynamic defence.

In response, Visa has embedded advanced security technologies across the ecosystem. The following milestones represent the foundational journey we have taken to secure digital commerce:

Implement strong customer authentication



Singapore achieved full enablement of EMV® 3-D Secure across eligible issuing products, strengthening eCommerce authentication. Visa also partnered with acquirers to upgrade merchant terminals to EMV® chip acceptance, aligning with contactless specifications and reinforcing the infrastructure for secure, low-friction payments.

Drive adoption of secure technologies



Building on this foundation, Singapore introduced tokenisation to replace sensitive card data with secure tokens. This enhanced digital transaction safety, improved authorisation performance, and prepared the ecosystem for broader adoption as market and regulatory readiness evolved.

Enhance fraud prevention and detection with real-time risk scoring



Visa Singapore advanced fraud prevention by deploying real-time risk scoring powered by AI. This shift to dynamic, data-driven models enabled instant anomaly detection, reduced false positives, and reinforced regulatory alignment - elevating trust in digital payments.

Strengthen partner accountability with TPA registration and Visa Integrity Risk Program (VIRP) rollout



Visa Singapore aligned its third-party and merchant risk oversight. These changes clarified agent roles, improved merchant risk visibility, and enabled acquirers to manage compliance more efficiently supporting scalable, secure growth across the ecosystem.

Maintain compliance with Account Information Security (AIS) Program and PCI DSS v4



Singapore maintained strong compliance with Visa's AIS Program and transitioned to PCI DSS v4. Streamlined validation, proactive remediation, and third-party oversight strengthened data protection and reinforced ecosystem integrity.



Lesson learnt

Strategic investment in technology enables future-ready security

Previous Visa Security Roadmaps have significantly shaped risk and security standards in Singapore's payments ecosystem. As new risks emerge with new opportunities in the era of generative artificial intelligence (GenAI), we look to the role that AI can play in secure technologies for the future. Visa has already invested US\$3 billion globally in AI and data infrastructure over the past decade³.

Collaboration is the cornerstone of sustainable security

Singapore's security journey has shown that meaningful progress comes from aligning innovation with ecosystem collaboration. Success was driven not only by technology upgrades but by engaging with regulators, acquirers, and third parties to ensure clarity, shared accountability, and operational feasibility. When risk and business priorities are jointly addressed, trust becomes a catalyst for sustainable growth.

³ Visa, AI: The Next Frontier, January 2025, <https://corporate.visa.com/en/sites/visa-perspectives/trends-insights/ai-the-next-frontier.html>

A changing world

The rapid change playing out in payments is the reflection of a changing world.

The COVID-19 pandemic accelerated the evolution of eCommerce in Singapore, pushing more consumers and businesses online and making digital trade a core part of everyday life. Recent national statistics show that the digital economy - driven by Information and Communications Technology (ICT) and e-commerce - contributed 18.6% (S\$128.1 billion) to Singapore's economy in 2024, growing faster than overall GDP.⁴

Singapore has emerged as one of Southeast Asia's fastest-growing digital economies (DE), with official data reporting that its overall DE grew at a compound annual growth rate (CAGR) of 12% value.⁴ This surge is expected to continue over the next few years as more Singaporeans shop, pay and run businesses online.⁵

However, greater digitalisation and the growing use of AI have increased the threat posed by cyberattacks, scams and other forms of cyber-enabled fraud. In 2025, close to S\$1 billion was lost to scams. Although the number of reported scam cases declined by 27.6% to 37,308 and total losses decreased by 17.9% to approximately S\$913.1 million compared with 2024, the overall impact remains deeply concerning. Combating scams therefore remains a key priority for the government.⁶

This is particularly important as commerce and payments continue to shift online, card-not-present fraud and authorised payment scams remain among the most damaging forms of fraud. Their persistence underscores the urgent need for coordinated action across the ecosystem to strengthen fraud prevention and detection, improve consumer education, and reinforce regulatory enforcement.

⁴ Singapore Digital Economy Report 2025, <https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches>

⁵ Google, Temasek & Bain, "e-Conomy SEA report 2025: Southeast Asia's digital economy." e-Conomy SEA 2023 report: Southeast Asia's digital | Bain & Company

⁶ SPF, Annual Scam and Cybercrime Brief 2025, <https://www.scamshield.gov.sg/resources/scams-and-cybercrime-briefs/>



Understanding the new threat landscape

As digital commerce accelerates, cybercriminals are evolving faster than ever—leveraging AI, automation, and global coordination to scale attacks. Visa’s 2026 global threat intelligence highlights six critical trends reshaping the payments ecosystem. These insights are essential for Singapore’s security roadmap as the region deepens its digital transformation.⁷



Scams Now Mirror Consumer behaviour in Real Time, with fraudsters targeting seasonal spending, tax refunds, and flash sales using fake offers and counterfeit promotions.



The Barrier to Becoming a Fraudster Has Hit an All-Time Low, as low-cost tools and automation make it easy for anyone to launch global scams from a mobile device.



AI-Powered Identity Attacks Are Accelerating. Deepfakes and synthetic IDs are now used to impersonate individuals and take over entire digital identities.



AI-Driven Scam Detection Is Becoming Core Infrastructure. Real-time AI is mapping fraud patterns and disrupting scams before they spread across markets.



Investment⁸ and Romance Scams Are Growing Rapidly, exploiting delivery alerts and emotional trust to deceive victims and cause financial harm.



Real-Time Collaboration Has Become the Deciding Factor, with cross-border data sharing and industry coordination now essential to stop organised fraud.

⁷ Visa, “6 Security Trends Shaping the Payments Ecosystem in 2026,” January 2026. <https://corporate.visa.com/en/sites/visa-perspectives/security-trust/6-security-trends-shaping-the-payments-ecosystem.html>

⁸ SPF, Annual Scam and Cybercrime Brief 2025. <https://www.scamshield.gov.sg/resources/scams-and-cybercrime-briefs/>

Changing Fraud and Scam Landscape in Singapore



Navigating Singapore's Evolving Fraud Landscape

Singapore's payment landscape continues to evolve, shaped by rapid digital adoption and shifting consumer behaviours. Fraud is adapting in response moving beyond **unauthorised card use** toward **authorised payment scams** that exploit trust and urgency. Visa 2025 regional trends highlights Singapore's exposure to **token provisioning fraud** and **scam-driven attacks**, which are increasingly linked to behavioural manipulation rather than technical compromise. These trends underscore the need for **risk strategies that are dynamic and user-centric**, balancing protection with seamless payment experiences.



Escalation in Online and CNP Fraud

In 2025, **CNP fraud** represented the **largest source of fraud losses in Singapore**, driven by rapid e-commerce growth and tactics such as phishing, impersonation and malware. Visa Asia Pacific data shows **Singapore's CNP fraud rate reached 16.2 basis points**, versus an **Asia-Pacific average of 11.7 basis points**.⁹ **Cross-border fraud** remains the main source of losses, indicating tighter domestic controls but a shift in attack surfaces. Despite these challenges, the Anti-Scam Command (ASC) recovered over S\$140.5 million of scam losses in 2025, reflecting ongoing efforts by law enforcement and industry stakeholders to combat scams and strengthen consumer protection.¹⁰



GenAI-Driven Scam Innovation

While the use of **GenAI** in fraud has been widely discussed, Visa 2025 threat intelligence adds nuance to its impact. Beyond synthetic content, GenAI is now being used to **automate reconnaissance, customise scam narratives**, and **scale social engineering** with precision. These developments are particularly relevant in Singapore, where **investment, romance and government official impersonation scams (GOIS)** have become increasingly sophisticated. Rather than viewing GenAI solely as a threat, it also presents an opportunity for the industry to **advance detection capabilities**, foster **cross-functional collaboration**, and explore **AI-driven risk modelling** to stay ahead of adversaries.



Data Breaches and Cybersecurity Risks

The rise in data breaches, which surged nearly 142% in 2025¹¹, continues to undermine Singapore's digital ecosystem as large-scale leaks grow more frequent and damaging. Visa global monitoring identified a significant uptick in **ransomware and breach activity**, with a growing focus on **supply chain vulnerabilities**. In Singapore, this reinforces the importance of **cyber hygiene, incident response readiness**, and **secure merchant integration**.

⁹ Visa, 12 months ending December 2025. Fraud rates are from the issuing perspective.

¹⁰ SPF, Annual Scam and Cybercrime Brief 2025. <https://www.scamshield.gov.sg/resources/scams-and-cybercrime-briefs/>

¹¹ The Straits Times, The Cyber Security Agency of Singapore: <https://www.straitstimes.com/tech/systems-infected-by-malware-in-spore-more-than-double-in-2025-csa>

National Drive Against Scam and Cyber Fraud Threats

In response to these challenges, initiatives have been launched across sectors in Singapore to combat fraud and scams and address data security issues. These include:¹²

- The SPF has expanded **ScamShield** suite since its launch in November 2020, comprising an AI-enabled mobile app that checks, filters and blocks scam SMS/calls, a one-stop website, and a 24/7 helpline to support verifications and interventions. It also established the Anti-Scam Command Office (ASCom) in September 2022 to centralise disruptions to scam operations and coordination of responses with financial institutions (FIs), telcos and e-commerce platforms.
- MAS launched **Project MindForge** in 2023 as a multi phase industry initiative to develop a comprehensive generative AI risk framework and strengthen responsible deployment across the financial sector. Phase 1 set out a **White Paper on the Emerging Risks and Opportunities of Generative AI for Banks**, outlining seven risk dimensions as guidance in building capabilities. Phase 2 is ongoing and includes traditional AI and agentic AI, and the insurance and asset management sectors. MAS has also published the **AI Risk Management Executive and Operationalization Handbooks** ahead of upcoming supervisory expectations.
- In February 2025, the Association of Banks in Singapore (ABS) announced an **enhanced card provisioning process**¹³ where it required major card issuing banks to require additional verification for provisioning of cards into mobile wallets. These measures have made it more difficult for a scammer to provision a customer's card into a mobile wallet.
- In December 2024, the **Shared Responsibility Framework (SRF)** was introduced by the Monetary Authority of Singapore (MAS) and Infocomm Media Development Authority (IMDA) to set clear duties for financial institutions and telecommunication companies in mitigating phishing scams for account transfers.
- In October 2024, the revised **E-Payments User Protection Guideline (EUPG)** was released to set out responsibilities for financial institutions and consumers on unauthorised and erroneous payment transactions, and establish baseline protection offered to consumers for losses from such transactions.
- From July 2025, under the **Protection from Scams Act**, the SPF can now issue Restriction Orders to banks for up to 30 days where there is reasonable belief that an individual is at imminent risk of transferring funds to scammers. This last resort measure kicks into place when other intervention measures have been exhausted.
- Launched in June 2024, the **Global Anti-Scam Alliance (GASA) Singapore Chapter** has become an important platform for collaboration against scams. Visa's appointment to the board in February 2026 reflects the strength of our expertise and our commitment to collective action. Together, these partnerships underscore the value of trusted intelligence-sharing and coordinated action against evolving scam threats.



¹² BGA Singapore, National Drive Against Scams and Cyber Fraud, prepared for Visa.

¹³ Association of Banks in Singapore, "Major Card Issuing Banks to Step Up Measures to Combat Card Provisioning Scams," 17 February 2025, <https://abs.org.sg/docs/library/major-card-issuing-banks-to-step-up-measures-to-combat-card-provisioning-scams.pdf>

Visa Security Roadmap

2026 and Beyond

Taking this changing landscape into account, this latest edition of Visa's Security Roadmap outlines six focus areas to strengthen resilience in the payment ecosystem into 2026 and beyond.

-
- 1** Strengthening cybersecurity to anticipate emerging threats & enhance ecosystem resilience
 - 2** Advancing authentication for a seamless & secure digital experience
 - 3** Enabling safer transactions with tokenised payments
 - 4** Transforming eCommerce checkout to enhance consumer confidence & convenience
 - 5** Leveraging foundational standards to drive network performance
 - 6** Building a resilient payments ecosystem to combat fraud and scams in the AI era
-



1

Strengthening cybersecurity to anticipate emerging threats & enhance ecosystem resilience

The evolving threat landscape presents numerous challenges, with data breaches being a significant concern for Singaporeans.

In 2025, the Cyber Security Agency of Singapore (CSA) recorded 165 ransomware cases, a 4% year-on-year increase, alongside approximately 284,300 infected systems, up 142% from 2024, within Singapore's broader cyber threat landscape.¹⁴ These trends underscore growing systemic pressure on organisations, as persistent botnet activity, exploitation of unpatched infrastructure, AI-enabled ransomware and identity-based attack vectors continue to elevate the risk of data compromise and operational disruption across digital environments.

Visa Payment Fraud Disruption observed that while opportunistic attacks declined, **targeted breaches became more damaging**, leveraging exfiltrated data for extortion and resale. This trend underscores the critical need for robust vendor oversight especially as organisations increasingly rely on third-party agents for payment processing and data management.

In response to rising cyber threats, Visa is actively enhancing its cybersecurity defences across the payment ecosystem. Through strategic consultations and targeted risk assessments, Visa is implementing robust mitigation strategies to counter ransomware, phishing, and third-party vulnerabilities. Key initiatives include advanced threat intelligence, real-time fraud detection, and expanded industry training via the Payment Cybersecurity Institute.

Visa's commitment to Cyber Security and Resilience



Visa prioritises transaction security through strong governance and risk alignment with its business strategy. It actively monitors and reports cyber threats, sharing updates via security alerts and biannual global threat reports to protect the payment ecosystem. This is reinforced by robust Business Continuity Planning (BCP) and operational resilience capabilities designed to sustain or restore critical services during disruptions, while enabling coordinated response, timely decision-making and operational adaptability.

Visa Network Defense (VND) delivers real-time, network-level fraud detection to stop large-scale attacks before they reach consumers. By analysing billions of transactions across ATM, CNP and Point of Sales (POS) channels, VND detects anomalies and blocks threats instantly minimising losses, reducing regulatory risk, and protecting brand trust. It also offers actionable intelligence, 24/7 monitoring, and emergency support to strengthen the payment ecosystem.

Payment Card Industry Data Security Standard (PCI DSS) compliance is mandatory for all entities storing, processing or transmitting Visa account data. PCI DSS provides the technical and operational requirements for financial institutions, merchants and service providers to protect against attacks aimed at stealing cardholder data.

¹⁴ Cyber Security Agency of Singapore, Singapore Cyber Landscape 2025/2026: [Singapore Cyber Landscape 2025/2026](#) | [Cyber Security Agency of Singapore](#)

Across the payment ecosystem, there is an increasing trend for organisations to use third-party vendors or agents (TPAs) to scale their business. Visa's **Third-Party Agent (TPA) Registration Program** plays a vital role in ensuring adherence to Visa's rules and policies when TPAs are involved. These standards are pivotal in managing TPA relationships across the ecosystem, ensuring compliance, promoting integrity, and minimising risk.

From 2025–2026,

Data breaches increasingly occur through trusted partners and have exposed significant volumes of Singaporeans' personal data.¹⁵



The rise in the number of data breaches highlighted the ongoing third-party vendor risks.

As a result, stakeholders in the ecosystem are encouraged to conduct requisite due diligence and register TPAs with Visa¹⁶.

Visa's **Account Information Security Program (AIS)** is a global compliance programme dedicated to maintaining the safety and integrity of the Visa payment ecosystem.¹⁷ This is achieved through monitoring compliance and addressing security deficiencies to prevent compromise of Visa account data.

Visa has transitioned to a more streamlined merchant PCI DSS compliance reporting approach. This shift is designed to help provide acquirers with greater control and autonomy in overseeing and managing their merchants' compliance with PCI DSS requirements. Visa will shift its focus to non-compliant merchant cases and will continue to work with acquirers that have merchants under remediation.¹⁷

Part of Visa's consulting arm aids issuers in identifying system weaknesses through the **Visa Payment Threats Lab (VPTL)**. This solution proactively detects potential vulnerabilities within payment systems, ideally before they are targeted by malicious actors. Typically, such security gaps only come to light following a fraudulent incident, but with VPTL, issuers can recognise and rectify gaps and vulnerabilities in advance.

AI-Driven Cyber Defense (VVAH)

Visa's open-source Visa Vulnerability Agentic Harness (VVAH) uses AI agents to continuously identify, prioritise, remediate, and validate vulnerabilities, helping security teams operate at machine speed while maintaining human oversight and governance.

¹⁵ Cyber Security Agency of Singapore, Singapore Cyber Landscape 2025/2026. [Singapore Cyber Landscape 2025/2026 | Cyber Security Agency of Singapore](#)

¹⁶ To maintain transparency Visa established the public listing of service providers and their current PCI DSS validation status for all ecosystem participants. www.visa.com/onthelist

¹⁷ Visa, Account Information Security Program and PCI, accessed November 2024. <https://corporate.visa.com/en/resources/security-compliance.html#1>

Advancing authentication for a seamless & secure digital experience

Authentication (EMV® 3DS) continues to play a critical role in Singapore's digital payment security strategy by enabling adaptive, risk-based authentication. With richer data elements and enhanced decisioning capabilities compared to 3DS 1.0, issuers can better assess transaction risk and reduce unnecessary customer friction—supporting a safer and more seamless eCommerce experience.

The transition to protocol version 2.2.0 has improved usability across browser, in-app, and requestor-initiated channels. This supports consistent authentication flows and strengthens fraud prevention across devices, aligning with Singapore's push for secure, low-friction digital payments.

However, as phishing and social engineering scams escalate across the Singapore market, threat actors are increasingly exploiting weaknesses in static identity verification methods. Sole reliance on SMS-based One-Time Passwords (OTPs) introduces vulnerabilities that are actively targeted:

- **OTP Bypass Scams:** Threat actors can exploit OTPs to fraudulently provision payment accounts to their digital wallets or authenticate online transactions.
- **Relay Schemes:** In OTP relay schemes, the OTP is intercepted and used by fraudsters to authenticate transactions.
- **Rapid Monetisation:** Provisioning fraud often manifests as rapid monetisation of fraudulently provisioned tokens by threat actors, which creates a steep fraud curve.

In response to these threats, regulators in certain jurisdictions have responded to these threats by directing financial institutions to move away from SMS one-time passwords for authentication, and to implement alternative multi-factor mechanisms that are inherently less susceptible to social engineering attacks¹⁸.

For merchants and acquirers Visa introduced the **Visa Secure minimum data requirements** in August 2024 where merchants must provide required data in the authentication request.¹⁹

To address phishing risks, the Monetary Authority of Singapore (MAS) worked with major banks to phase out the use of One-Time Passwords (OTPs) for bank account login by customers who are digital token users. This is part of a shift towards more secure authentication methods such as in-app authentication.

A consistently high quantity and quality of data fields help enhance business outcomes for merchants, cardholders and issuers.

Incorporating **biometric authentication with tokenisation** can greatly enhance the security of online transactions by ensuring consumers are accurately verified. Technologies such as **Passkeys** further strengthen this approach, allowing cardholders to authenticate online transactions using biometrics or device-based cryptographic keys in place of passwords or SMS one-time passwords where both methods are often vulnerable to phishing and social engineering attacks.

These capabilities will be integrated across Visa's existing product suite and programmes, enabling a consistent, seamless, and more secure authentication experience for cardholders.

¹⁸ Banks in Singapore to phase out login OTPs for digital token users. CNA, 9 July 2024 <https://www.channelnewsasia.com/singapore/banks-phase-out-otps-login-phishing-scams-digital-tokens>

¹⁹ Visa, Payer Authentication Data Fields in Relation to Visa Secure Program Guide Updates, 17 September 2024, [Payer Data Fields](#)

3

Enabling safer transactions with tokenised payments

Visa has issued more than

1.9 Billion

tokens in the Asia Pacific region boosting digital payments while enhancing security.²⁰



5%

Authorisation Rate Lift²⁰
Global Average for Visa
Token CNP transactions



39%

Fraud Reduction
Visa Token vs PAN-based
CNP transactions²¹

Tokenisation replaces a 16-digit debit or credit card number with a unique identifier, a token, that only Visa can unlock. Visa tokens secure the payment credential, enabling the transfer of enhanced data, which can help to improve payment success rates and lower fraud rates. These benefits, coupled with ease of use across devices, lead to an improved consumer experience. The token devalues sensitive card data as it has no intrinsic or exploitable value and cannot be mathematically reversed to reveal the original card number. This remains one of the most secure ways to protect against card data compromise by removing it from the transaction flow and limiting the risk exposure in a breach.

In Singapore, token penetration rate is at

357 Million²²

99% of transactions are tokenised²¹

Token provisioning challenges

While tokenisation secures card data, its effectiveness depends on how tokens are provisioned. Fraud can occur when tokens are activated by bad actors - especially in device-bound wallets. In 2022, global losses from token provisioning fraud reached **USD 450M**²¹. In Asia Pacific, provisioning fraud has generally decreased, but it is still being monetised at a later date.²¹

To combat this, Visa launched **Visa Provisioning Intelligence (VPI)**, an AI-based solution designed to combat token provisioning fraud at its source, which uses machine learning to rate the likelihood of fraud for token provisioning requests. This helps financial institutions prevent fraud in a targeted way and enables more seamless and secure transactions for Visa cardholders. VPI is designed to help reduce overall ecosystem fraud and increase the number of valid token provisioning requests.

²⁰ VisaNet, Jan-Dec 2024. Visa credit and debit card-not-present transactions for tokenised vs non-tokenised credentials in the AP region. Auth rate is defined as approved authorisations divided by total authorisation attempts based upon first attempt of a unique transaction.

²¹ Visa Risk Datamart, Global, FY24 Q1-Q4 Token Fraud Rate vs PAN Fraud Rate by PV. Merchant rates may vary.

²² Visa internal data transaction data from Q3 2025



As the industry strengthens authentication at checkout and account access through Passkeys and EMV 3-D Secure, fraud pressure has shifted elsewhere. With the rapid adoption of tokenised mobile wallets, attackers increasingly target the wallet provisioning stage, using phishing and social engineering to bypass controls upstream. As a result, secure token provisioning has become the new baseline, making strong authentication and intent verification at enrolment critical to protecting mobile wallet usage at scale.

Singapore Case Study: Baseline Controls for Mobile Wallet Provisioning²³

Mobile wallets are widely used in Singapore, offering convenience but also expanding the attack surface at the point of card provisioning.

Following a rise in phishing-enabled scams involving the fraudulent provisioning of cards into mobile wallets, Singapore authorities and industry bodies introduced baseline controls to strengthen authentication and intent verification during enrolment, without undermining user experience.

Under Singapore's industry-led and regulator-supported approach, the **Baseline Controls for Mobile Wallet** Provisioning define the minimum security and authentication requirements that key card-issuing banks must implement when allowing cards to be added to mobile wallets.

Coordinated primarily through the Association of Banks in Singapore (ABS), with support from the Monetary Authority of Singapore (MAS), the controls aim to prevent unauthorised provisioning, particularly where attackers socially engineer victims into disclosing SMS OTPs during wallet enrolment.

Singapore's Baseline Controls for Mobile Wallet Provisioning adopt a layered approach to strengthening authentication across the provisioning lifecycle, addressing risks associated with phishing-enabled card enrolment into mobile wallets.



1. Prevent: Time-bound provisioning with digital token / in-app authentication



2. Detect: Identify and de-provision cards from rogue devices

Together, these measures advance authentication beyond credentials alone, supporting both security and a seamless digital payment experience.

As an additional layer, Visa supports secure mobile wallet provisioning through tokenisation and device-binding, ensuring card details are never shared and transactions remain protected even if a device is compromised.

²³ Association of Banks in Singapore, "Major Card Issuing Banks to Step Up Measures to Combat Card Provisioning Scams." <https://abs.org.sg/docs/library/major-card-issuing-banks-to-step-up-measures-to-combat-card-provisioning-scams.pdf>

Transforming eCommerce checkout to enhance consumer confidence & convenience

Digital payments are transforming how Singaporeans shop and transact - and the checkout experience has become a critical point for both trust and conversion.

Every new experience Visa introduces is built to deliver seamless convenience without compromising security. Our latest innovations strengthen trust while making online and in-store payments faster, simpler and safer.



One such innovation is Visa **Click to Pay (CTP)**, built on EMV® Secure Remote Commerce (SRC) specifications. Click to Pay addresses checkout friction by reducing manual card entry and minimising exposure of sensitive card data through tokenisation and secure authentication. Consumers can complete transactions with fewer steps, without repeatedly entering Primary Account Numbers (PANs) or card details across different merchants and devices.

Click to Pay delivers a consistent checkout experience across participating merchants and platforms, helping improve conversion rates while maintaining strong security controls. For merchants, it supports authenticated transactions using network and issuer-enabled security standards, reducing reliance on vulnerable data entry methods. Click to Pay supports an Issuer's preferred authentication methods including 3D Secure and Visa Payment Passkeys during the Click to Pay checkout experience.

Click to Pay directory supports partner checkout use cases, card on file, and may act as a secure onramp for cards enrolled in agentic buying experiences.



So with Click to Pay, consumers' cards are ready for checkout wherever and however they shop online or in app - simple, authenticated, and secure.





Visa is introducing next-generation checkout experiences to deliver flexibility, security, and convenience for Singaporean consumers and businesses.

Globally, Visa has announced the introduction of **Visa Flexible Payment (Flex)**, expanding the eCommerce checkout experience by giving consumers greater control over how and when they pay. Flex enables cardholders to choose from eligible payment options—such as instalments or deferred payments—based on issuer-defined parameters and consumer preferences.

When presented at checkout, Visa Flex integrates seamlessly into the payment flow without increasing complexity or compromising security. Consumers benefit from greater transparency and payment choice, while merchants can offer flexible payment options within existing acceptance and risk frameworks.

From a security perspective, Flex operates within Visa's network and issuer-led controls, ensuring transactions continue to be protected using tokenisation, authentication, and EMV-aligned standards. This approach supports improved authorisation performance while maintaining strong fraud protections.

Together, Click to Pay and Visa Flexible Payment simplify the eCommerce checkout journey by reducing friction, minimising exposure of sensitive data, and enhancing consumer confidence. These capabilities support Singapore's evolving digital commerce landscape with the right balance of convenience, security, and payment flexibility.

Leveraging foundational standards to drive network performance

Strengthening the Payment Ecosystem through Unified Risk and Security Programmes.

Visa continues to enhance the integrity, security, and efficiency of the global payment system through a coordinated set of programmes and frameworks. These initiatives address every stage of the payment journey — from credential protection and authentication to fraud detection, reporting, and merchant risk management — ensuring that issuers, acquirers, merchants, and partners can operate with confidence and resilience.

The following is a non-exhaustive list of programmes and updates that form the foundation of this effort:

²⁴ Visa, Account Information Security Program and PCI, accessed November 2024, <https://corporate.visa.com/en/resources/security-compliance.html#1>

²⁵ Visa, Visa Core Rules and Visa Product and Service Rules, section 10.4.7.1, "Visa Issuer Monitoring Program (VIMP)," 18 April 2026, <https://corporate.visa.com/content/dam/VCOM/download/about-visa/visa-rules-public.pdf>

²⁶ Visa, Acceptance Risk Standards, 1 October 2024, <https://www.visa.com.sg/dam/VCOM/download/merchants/visa-global-acquirer-risk-standards.pdf>

Apr'21



The Network Performance Drive (NPD) introduced foundational frameworks to support secure and seamless payment experiences:

Secure Credential Framework (SCF) guidelines for protecting payment credentials in digital environments.

Digital Authentication Framework (DAF) encourages low-friction, robust authentication methods.

The streamlined **merchant** Payment Card Industry Data Security Standard (**PCI DSS**) requirements²⁴.

Aug'24



Updated **Visa Acceptance Risk Standards (VARs)** to help acquirers strengthen security, streamline operations, and collaborate more effectively²⁶.

Oct'24



Fraud Reporting and Control Program (FRECO) issuers must report fraud accurately.

Apr'25



Redesigned **Visa Integrity Risk Program (VIRP)** to better detect and manage illegal or miscoded transaction activity through enhanced case management tools.

Token Lifecycle Management All VTS issuers must ensure token data—account numbers and expiry dates—up to date.

Jun'25



Visa Acquiring Monitoring Program (VAMP) redesign to better capture fraud and dispute data into a single, more accurate risk metric.

Aug'25



Updated requirements on Fraud Reporting Systems to include **confirmed fraud on declines** for better model development and to support issuers in making smarter risk-based decisions that drive down fraud.

Introducing Merchant Elevated Risk Program (MERP) to target objective elevated merchant risk activity and an avenue for liability reversal and reimbursement for issuers and cardholders.

Apr'26



Visa Issuer Monitoring Program (VIMP)²⁵

Fraud Reporting and Control Program (FRECCOP)

As part of Visa's continued efforts to secure the payments ecosystem, the new Fraud Reporting and Control Program (FRECCOP) was launched to help ensure accurate and complete fraud reporting from all issuers globally.

High-quality fraud reporting is essential for effective risk management across the ecosystem. Accurate data enables issuers, acquirers, and Visa to better identify emerging fraud patterns, assess systemic risk, and apply targeted controls where needed.

Through FRECCOP, issuers are held accountable for consistent fraud reporting across confirmed fraud scenarios, supporting improved fraud analytics, stronger decision-making, and more effective ecosystem-wide risk mitigation. This enhances overall network performance while reinforcing consumer trust.



Visa Acquirer Monitoring Program (VAMP)

Due to the rapidly evolving payment ecosystem, Visa has also updated and strengthened acquirer risk controls for the new Visa Acquirer Monitoring Program (VAMP)²⁷.

VAMP has the potential to address

4x THE AMOUNT OF FRAUD GLOBALLY, ACCOUNTING FOR MORE THAN US\$2.5BN IN LOSSES,

compared to previous programmes and will help acquirers prevent fraudulent activities.

VAMP, effective 1 April 2025, creates more seamless controls and processes for acquirers and merchants to effectively deter fraud and enumeration and manage disputes, contributing to a more secure environment. The changes include:

Retiring the existing fraud and disputes monitoring programme to create globally aligned fraud thresholds for both domestic and cross-border CNP transactions.

Incorporating new enumeration criteria based on the number of enumerated authorisation transactions and the enumeration rate identified by the VAAI Score, which provides increased coverage on enumeration monitoring.

Launching the new risk technology tool Visa Ecosystem Risk Control (VERC), a case management tool that allows for independent portfolio performance monitoring and improves operational efficiency.

Visa Integrity Risk Program (VIRP)

To protect the integrity of the Visa payment system, Visa introduced the Visa Integrity Risk Program (VIRP) in 2023, with enhanced requirements effective 1 October 2025.

VIRP is designed to

DETER, DETECT AND REMEDIATE ILLEGAL ACTIVITY ACROSS THE ECOSYSTEM

helping acquirers and their agents maintain proper controls and oversight to prevent prohibited transactions.

The programme addresses growing threats such as illegal online gambling, counterfeit goods, prohibited pharmaceuticals, and transaction laundering.

Key changes include:

- Establishing globally aligned integrity benchmarks and mandatory registration for high-integrity risk merchants via the High Integrity Risk Registration (HIRR) module.
- Introducing proactive intelligence tools to monitor suspicious transactions and provide timely reporting for risk mitigation.
- Enforcing enhanced compliance for high-risk Merchant Category Codes (MCCs), including quarterly attestations and tiered oversight for categories like gambling, adult content, and crypto-related transactions.
- Launching the Visa Integrity Control Suite (VICS) for real-time risk scoring and automated remediation workflows.

²⁷ Visa, Introducing the Visa Acquirer Monitoring Program, 30 August 2024, <https://usa.visa.com/visa-everywhere/blog/bdjp/2024/08/29/introducing-the-visa-1724958906425.html>

Merchant Elevated Risk Program (MERP)

To maintain security, integrity and combat deceptive and fraudulent activity, Visa introduced the Merchant Elevated Risk Program (MERP) for acquirers effective 1 April 2026.²⁸

The Merchant Elevated Risk Program (MERP) is being introduced and designed to enhance Visa's risk coverage by targeting objective elevated merchant-risk activity and offering an avenue for liability reversal and reimbursement for issuers and cardholders. MERP concentrates on high-confidence cases of deceptive activity that manifest through smaller-scale, disproportionate fraud/dispute rates or abnormal spikes in activity.

MERP aims to:

- Identify merchants whose activity (e.g. fraud and dispute rates, decline rates or abnormal spikes in activity) demonstrates excessive risk.
- Improve acquirer controls and oversight to prevent, detect and remediate elevated-risk merchant activity.
- Enable issuer and cardholder reimbursement for losses resulting from fraudulent transactions at identified merchants.
- Strengthen the integrity of the Visa ecosystem by enhancing risk coverage and supporting safer commerce for all stakeholders.

²⁸ Visa, Introducing the Merchant Elevated Risk Program Merchant Elevated Risk Program - Visa Access [Merchant Elevated Risk Program - Visa Access](#)



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

Generative AI is growing fast and becoming more widely used, especially as Singapore's eCommerce sector expands. This creates new risks in the payments system. At the same time, AI is helping us improve how we detect and stop fraud - making money movement safer and more secure for Singapore consumers and businesses.

In Singapore, it's more important than ever to understand both current and new threats - whether they come from cyberattacks, fraud, or scams. This understanding helps us build strong strategies to reduce risks and protect the payments ecosystem.

Visa has been using AI in payments for over 30 years. In fact, we were the first network to use AI for real-time fraud detection back in 1993²⁹. Today, we run around 150 AI and machine learning models that support products designed to solve problems for consumers, merchants, and financial institutions.

These models help us tackle issues like CNP fraud and make authentication smoother and more secure. AI is a key part of how we build trust and resilience in Singapore's digital economy.

Looking ahead, Visa Singapore will continue to:

- Improve local threat detection and risk mapping;
- Work closely with regulators and partners across the ecosystem;
- Invest in security tools that work quietly in the background without affecting user experience; and
- Support local initiatives that address scam types unique to Singapore.



²⁹ Visa, Rajat Taneja, Visa: 30 years of AI and counting, September 2023, <https://usa.visa.com/visa-everywhere/blog/bdp/2023/09/13/30-years-of-1694624229357.html>



Unauthorised fraud

Visa [Zero Liability Policy](#) protects consumers from unauthorised transactions. In Singapore, fraud rose with the growth of eCommerce, especially in CNP transactions. Cross-border fraud drove most losses, while domestic fraud remained low due to strong local controls.

Visa scheme rules and AI-powered tools like Visa Protect suite help issuers detect fraud early and support merchants in improving CNP conversion. This is increasingly critical in Asia Pacific, where 2.6% of annual eCommerce revenue is lost to fraud—highlighting the need for smarter, data-driven prevention across the ecosystem.

Issuing fraud

Singapore's issuing fraud rate is above that of Asia Pacific (6.3 bps), highlighting a need for stronger controls.

 **8.3** bps in 2025³⁰

Key Merchant Category Code (MCC) Fraud Drivers



Advertising Services



Travel Agencies



Hotels / Resorts

CNP Fraud: Persistent, especially cross-border. Rates historically high but easing with EMV 3DS;

Synthetic Identity & Account Takeover: AI-driven identities exploit weak SMS OTP. Strengthen verification and adopt **biometrics/passkeys**.

Lost and Stolen Fraud: Risk persists from unauthorised use of physically stolen cards.

Acquiring fraud

Enumeration Attacks: Merchants and acquirers are prime targets for automated credential guessing. Visa mandates anomaly detection, throttling, and account lockout mechanisms for payment gateways and acquirers closest to the checkout page.

Collusive Merchants: Collusion and elevated-risk behaviours can lead to unauthorised transactions. Industry best practice is to strengthen merchant monitoring and apply robust liability frameworks.

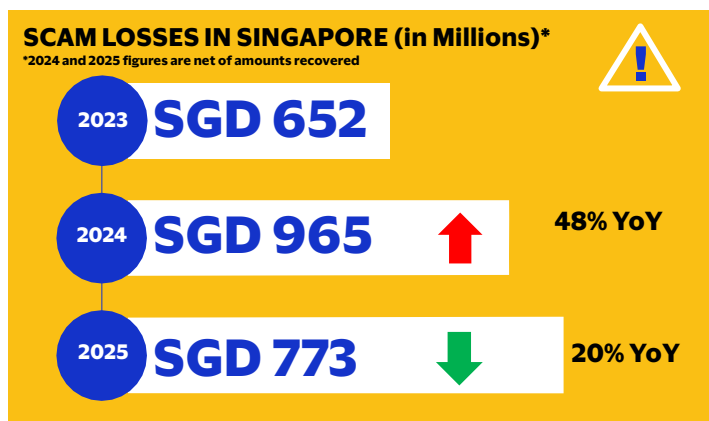
Cybersource enhances acquirer fraud defences with AI-driven detection and VisaNet intelligence. It mitigates **enumeration attacks** through device fingerprinting and pre-authorisation screening, monitors **merchant risk** using behavioural analytics, and secures **token provisioning** with multi-layer authentication and token integration. These capabilities support acquirers in lowering fraud exposure while enabling secure, seamless acceptance.

³⁰ Visa, 12 months ending December 2025. Fraud rates are from the issuing perspective.



Authorised payment (scams)

There is an increasing level of attention on scams as they continue to be a growing concern for all participants in Singapore's payment ecosystem.



SINGAPORE SCAM LANDSCAPE: 2025 SNAPSHOT

Highest loss by scam type

- Investment Scams 14.6% of victims lost money³¹
- Government Officials Impersonation Scams
- Employment Scams

Recovery Rate Only S\$140.5 Million was recovered out of S\$913.1 million in total scam loss³¹.

Visa Scam Mitigation Framework provides the strategic foundation for identifying, preventing, and responding to scams by aligning with regulatory expectations and protecting consumers across the payment ecosystem.

Visa Acceptance Risk Standards (VARs) operationalise this strategy by embedding fraud controls directly into acquiring processes, ensuring that merchants are properly vetted, monitored, and held to consistent risk standards.

Together, these frameworks create a unified defence against scams: one that spans from consumer protection and regulatory compliance to merchant accountability and ecosystem integrity, helping reduce fraud losses and enabling safer digital commerce in Singapore.

Visa Scam Disruption (VSD) complements these efforts by leveraging Visa's intelligence, analytics, and cross-ecosystem visibility to identify, investigate and disrupt scam networks before they can scale. By targeting scam enablers and supporting timely intervention, VSD strengthens Visa's ability to protect consumers and financial institutions from emerging scam threats.

Visa's expansion into **Real-Time Payments (RTP)** brings its advanced fraud tools—like **Visa Protect for Account to Account (VPAA)** into the heart of scam-prone **Authorised Push Payment (APP)** transactions, while its acquisition of **Featurespace** adds **real-time behavioural analytics** that detect anomalies at the account level. Together, they deliver predictive, AI-powered scam defence that empowers financial institutions to protect consumers and secure digital payments with greater precision and speed.

³¹ Singapore Police Force, Annual Scam and Cybercrime Brief 2025, <https://www.scamshield.gov.sg/resources/scams-and-cybercrime-briefs/>

Visa has actively participated in the creation of different initiatives and tools, contributing to a safer digital environment in Singapore.

We continue to put our technology and expertise to work to enhance security, reduce fraud, and deliver seamless digital experiences for Singaporean consumers and merchants. In addition, Visa has invested over US\$10 billion into technology and innovation in the last five years,³² to strengthen fraud prevention solutions and increase network security.

In 2024, we expanded Visa Protect, a suite of risk and identity products designed to safeguard consumers and businesses with new AI-powered solutions aimed at reducing fraud for transactions both on and off Visa's network. These include account-to-account and card-not-present payments. Key solutions within the Visa Protect suite include:

- Visa Advanced Authorisation (VAA), which utilises machine learning to provide real-time risk assessments for transactions, helping to identify and prevent fraud.
- Visa Consumer Authentication Service (VCAS), which enhances security for online transactions by providing secure authentication methods such as biometrics.
- Visa Provisioning Intelligence (VPI), which facilitates secure token provisioning to combat increasing token provisioning fraud.
- Visa Account Attack Intelligence (VAAI) Score is a real-time risk score that uses AI and generative AI components to identify the likelihood of account enumeration attacks in card-not-present (CNP) transactions. It helps issuers detect and block compromised payment credentials before they are used for fraud.
- Visa Protect for Account to Account (VPAA), which offers additional protection for account-to-account transactions.



Adaptive AI to outpace fraud: Featurespace's Real-Time Behavioural Analytics powers safer digital payments with Visa.

³² Visa, "Reimagining payments with Visa: Key trends shaping the future of 2025," <https://www.visa.com.ph/about-visa/newsroom/press-releases/reimagining-payments-with-visa-key-trends-shaping-the-future-of-2025.html>

Looking ahead

Visa will continue to engage our stakeholders and partners to meet the evolving needs of consumers and businesses, working together to secure the payment system in Singapore and globally.

Trust remains at the core of everything we do, and our collective responsibility is to continue to earn that trust by protecting individuals and businesses as the commerce landscape and threat environment evolves. Maintaining a secure payments ecosystem requires coordinated action across regulators, financial institutions, merchants, technology providers, consumers and payment networks, with every stakeholder playing a role in strengthening security and resilience. Together, we must drive security alongside payment innovation as we enable new and exciting ways to pay.

Considering these expectations of the Singapore threat landscape in the coming years, Visa has mapped the steps we are already taking with ecosystem partners during 2026 and into the coming years to highlight the critical areas for action.

2019



Implement strong customer authentication



Drive adoption of secure technologies



Enhance fraud prevention and detection with real-time risk scoring



Strengthen partner accountability with TPA registration and Visa Integrity Risk Program (VIRP) rollout



Maintain compliance with Account Information Security (AIS) Program and PCI DSS v4

2025



Accelerate adoption of secure, seamless payments with network token to boost approvals and reduce fraud



Detect and block large-scale fraud attacks and scams



Monitor fraud performance and reporting accuracy with VAMP and FRECOP



Strengthen merchant onboarding with updated Visa Acceptance Risk Standards (VARS) to block bad actors



Enhance consumer protection against scams

2026 and beyond



Conduct annual cyber posture assessments to ensure readiness



Shift from SMS OTP to biometric / in-app authentication, Visa Payment Passkeys and tokenisation to strengthen identity verification and reduce fraud



Streamline checkout through Click to Pay enablement to reduce card data exposure



Empower consumers with greater control



Call to action

ONE ECOSYSTEM, SHARED RESPONSIBILITY

Trust is Singapore's next growth currency. Securing the future of digital payments requires decisive leadership and collaboration across the ecosystem. To sustain this success and stay ahead of emerging threats, **every stakeholder must own their role in building resilient and enabling trust.**

Issuers – Lead the trust agenda



- ✓ Empower account holders with guidance on payment security and scam awareness.
- ✓ Enhance digital experience with mobile apps and wallets featuring **biometrics, alerts, and advanced security controls.**
- ✓ Reduce risk and improve user experience by **moving beyond SMS OTP to frictionless authentication solutions.**
- ✓ Optimise authorisation rates and combat fraud through **real-time decisioning and AI-driven risk intelligence.**
- ✓ **Secure** all payment rails, including account-to-account, with tokenisation and card data safeguards to prevent scams.

Regulators – Shape the future



- ✓ Enable **responsible AI frameworks** for fraud detection and data sharing.
- ✓ Promote **consumer-centric controls** to accelerate safe digital adoption.

Consumers – Empower the end-user



- ✓ **Take control of payment security** by keeping your contact details up to date and enabling mobile alerts.
- ✓ **Stay informed and vigilant** to prevent scams.
- ✓ **Protect your identity** by using secure authentication and never sharing sensitive information.

Acquirers – Turn security into growth



- ✓ Drive secure growth through strong merchant onboarding and collaboration with gateways to ensure seamless integration and risk resilience.
- ✓ **Enable tokenisation and Click to Pay** to drive conversion and loyalty.
- ✓ Equip merchants with advanced fraud tools to safeguard payment rails.
- ✓ Maintain oversight of third-party cyber health and implement contingency plans to safeguard business continuity.

Third-Party Service Providers – Innovate for scale



- ✓ Ensure PCI DSS compliance to protect payment data and maintain trust.
- ✓ Register with Visa as a Third-Party Agent to demonstrate commitment to global standards.
- ✓ Deliver fraud and risk management solutions using advanced authentication and tokenisation.

Merchants – Secure Payments



- ✓ Strengthen payment channel protection and reputation by **deploying advanced risk solutions and AI-driven fraud intelligence.**
- ✓ Drive business performance by **adopting secure technologies** – tokenisation, payment passkeys and frictionless authentication – to increase approval rates and reduce fraud.
- ✓ Deliver seamless onboarding and robust dispute management to build consumer trust and operational excellence.
- ✓ Work with acquirers to enable tokenisation for both card-on-file transactions and guest checkout (via Click to Pay).

A photograph of a young couple sitting on a rooftop or balcony at night. The woman is holding a smartphone, and both are smiling and looking at the screen. The background shows a city skyline with lights.

Together, we navigate tomorrow with confidence enabling trust at every transaction and driving success across Singapore's digital economy.

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