VISA

Security Roadmap

Thailand

2025–2028

November 2025

Contents

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 advise 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.

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.

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 three 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 and regulatory shifts
- Advancing authentication for a seamless experience
- Enabling safer transactions with tokenised payments
- Transforming eCommerce checkout to enhance consumer confidence and ease
- Leveraging foundational standards to drive network performance
- Building a resilient payments ecosystem to combat unauthorised fraud and authorised payment scams

- 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
150M
MERCHANT LOCATIONS

4.8B
PAYMENT CREDENTIALS

US$16.4T
IN TOTAL VOLUME

322.4B
TOTAL TRANSACTIONS
in its fiscal year 2025[1]

[1] Visa Fact Sheet, June 2025, https://corporate.visa.com/content/dam/VCOM/corporate/visa-perspectives/documents/about-visa-factsheet.pdf

The journey

Since our first Visa Thailand Security Roadmaps in 2018 and its successor 2022, 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

Thailand 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, Thailand introduced credit 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

Thailand 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

Thailand 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

Thailand 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

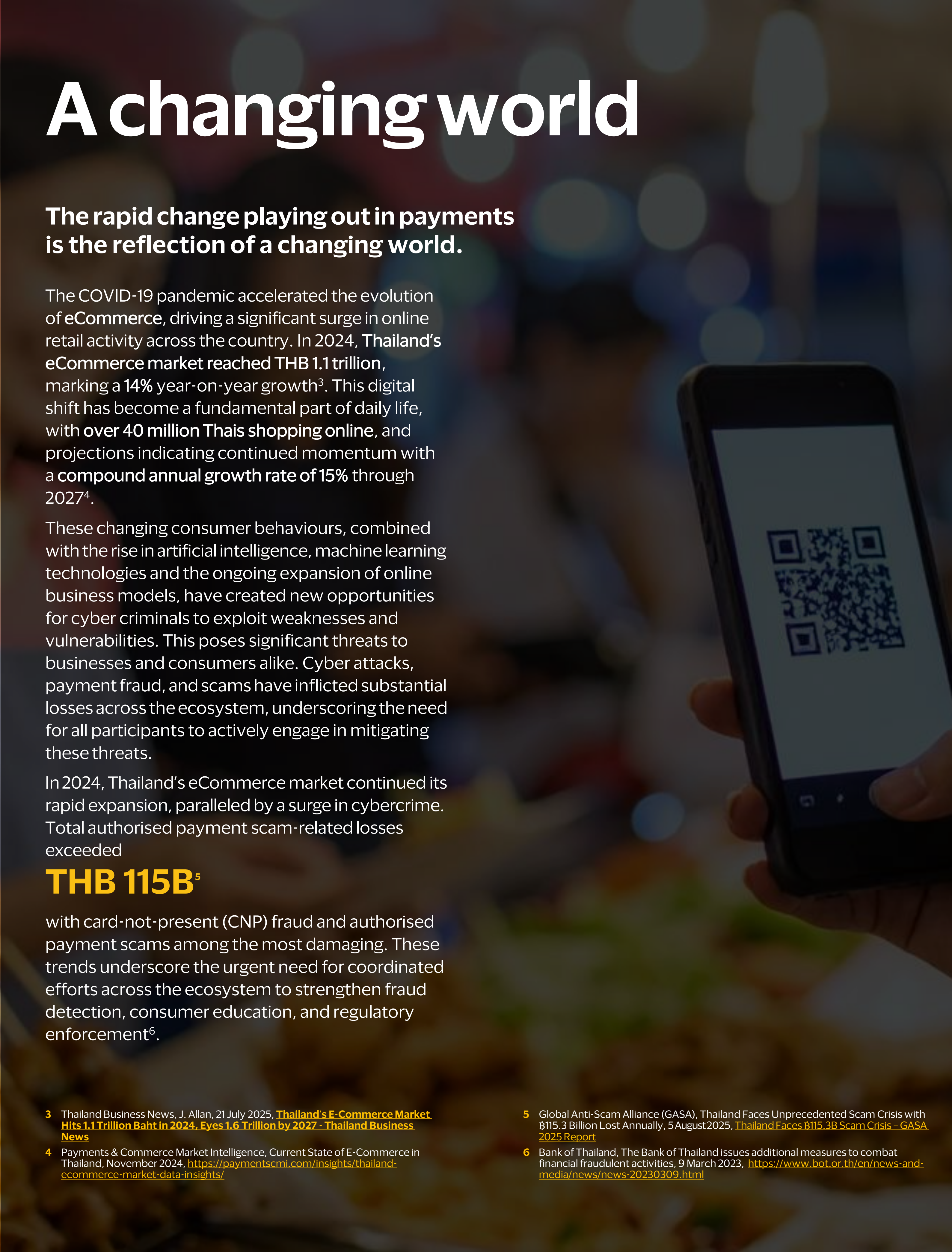
Strategic investment in technology enables future-ready security

Previous Visa Security Roadmaps have significantly shaped risk and security standards in Thailand'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 decade**[2].

Collaboration is the cornerstone of sustainable security

Thailand'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.**

[2] 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**, driving a significant surge in online retail activity across the country. In 2024, **Thailand's eCommerce market reached THB 1.1 trillion**, marking a **14%** year-on-year growth[3]. This digital shift has become a fundamental part of daily life, with **over 40 million Thais shopping online**, and projections indicating continued momentum with a **compound annual growth rate of 15%** through 2027[4].

These changing consumer behaviours, combined with the rise in artificial intelligence, machine learning technologies and the ongoing expansion of online business models, have created new opportunities for cyber criminals to exploit weaknesses and vulnerabilities. This poses significant threats to businesses and consumers alike. Cyber attacks, payment fraud, and scams have inflicted substantial losses across the ecosystem, underscoring the need for all participants to actively engage in mitigating these threats.

In 2024, Thailand's eCommerce market continued its rapid expansion, paralleled by a surge in cybercrime. Total authorised payment scam-related losses exceeded

THB 115B[5]

with card-not-present (CNP) fraud and authorised payment scams among the most damaging. These trends underscore the urgent need for coordinated efforts across the ecosystem to strengthen fraud detection, consumer education, and regulatory enforcement[6].

[3] Thailand Business News, J. Allan, 21 July 2025, **Thailand's E-Commerce Market Hits 1.1 Trillion Baht in 2024, Eyes 1.6 Trillion by 2027 - Thailand Business News**

[4] Payments & Commerce Market Intelligence, Current State of E-Commerce in Thailand, November 2024, https://paymentscmi.com/insights/thailand-ecommerce-market-data-insights/

[5] Global Anti-Scam Alliance (GASA), Thailand Faces Unprecedented Scam Crisis with ฿115.3 Billion Lost Annually, 5 August 2025, Thailand Faces ฿115.3B Scam Crisis – GASA 2025 Report

[6] Bank of Thailand, The Bank of Thailand issues additional measures to combat financial fraudulent activities, 9 March 2023, https://www.bot.or.th/en/news-and-media/news/news-20230309.html

Understanding the new threat landscape

The democratisation of technology has made tools and knowledge easier for people to access and, while this has delivered numerous social and economic benefits, it has also empowered cyber criminals, providing them with more opportunities and new channels for digital crime.

Compounded with Thailand's eCommerce growth and the variety of available payment options, the threat landscape has become increasingly complex. Visa's Payment Ecosystem Risk & Control teams have tracked several trending tactics repeatedly over the past 24 months[7]:

Increased adoption of AI by malicious actors, enabling voice cloning, deepfake impersonation, and highly targeted phishing and scam campaigns.

Synthetic identity fraud, with AI-generated identities used to bypass KYC and exploit merchant onboarding for account-based fraud.

High-speed, scalable attacks, including enumeration and PRA fraud, with threat actors leveraging automation to execute complex operations.

Exploitation of payment flow vulnerabilities, such as digital skimming via malicious code injection into merchant checkout pages.

Consumer-targeted scams, using fake mobile apps, task-based fraud, and non-traditional payment methods to monetise deception.

Persistent ransomware and breach activity, with attackers increasingly targeting third-party service providers to amplify impact.

[7] Visa, Biannual Threats Report, October 2025, https://corporate.visa.com/en/sites/visa-perspectives/security-trust.html

Navigating Thailand's Evolving Fraud Landscape

Thailand'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 2024 regional data highlights Thailand'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 2024, **CNP fraud** represented the **largest share of fraud losses in Thailand**, driven by the continued expansion of e-commerce and evolving fraudster tactics such as phishing, impersonation, and malware targeting digital channels. Visa Asia Pacific data shows **Thailand CNP fraud rate reached 37.3 basis points**, marking a **34% YoY increase**. This compares to the **Asia Pacific regional average of 35.8 basis points**, which rose by **5% YoY**[8]. **Cross-border fraud** remains the dominant source of losses, indicating stronger domestic controls but also a shift in attack surfaces. Regulatory actions, including the **freezing of nearly 300,000 mule accounts** since late 2023[9], reflect a more agile and coordinated approach to fraud disruption, helping reinforce consumer trust in digital payments

GenAI-Driven Scam Innovation

While the use of **GenAI** in fraud has been widely discussed, Visa 2024 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 Thailand, where **investment and romance scams** have shown increased sophistication. 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 up 19% in H2 2023 continues to challenge the integrity of digital ecosystems[10]. Visa global monitoring identified a significant uptick in **ransomware and breach activity**, with a growing focus on **supply chain vulnerabilities**. In Thailand, this reinforces the importance of **cyber hygiene**, **incident response readiness**, and **secure merchant integration**. Visa's recent updates to fraud reporting allowing issuers to flag **confirmed fraud on declined transactions** are helping to surface previously hidden threats, enabling **earlier intervention** and more **granular risk visibility** across the payment lifecycle.

[8] Visa, 12 months ending March 2025, VisaNet, January 2023 to December 2024.
[9] Biocatch, Thailand shuts down 200K mule accounts in two months: A good first step but much more needed
[10] Visa, Biannual Threats Report, October 2025, https://corporate.visa.com/en/sites/visa-perspectives/security-trust.html

National Drive Against Scam and Cyber Fraud Threats

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

- Establishment of the **Anti-Call Center Scam Centre** in February 2022, led by the Ministry of Digital Economy and Society (MDES) and the Royal Thai Police, to enhance rapid response to scam reports via hotline 1441 and an online portal. The initiative enables swift coordination with banks and telecom providers to block fraudulent accounts and phone numbers[11].
- Approval of the **Digital ID Framework Phase 2** in November 2024, expanding secure digital identity services to foreigners and legal entities, with a goal of enabling 1,000 e-services by 2027[12].
- Announcement of Thailand's **Shared Responsibility Framework (SRF)** in December 2024, which outlines joint obligations for financial institutions and telecommunication operators in scam prevention and victim remediation, inspired by Singapore's model[13].
- Implementation of **Cybersecurity Act Notifications** in January 2025, setting minimum standards for data protection and risk-based classification across critical infrastructure sectors[14].
- Draft **Digital Fraud Management Guidelines** by the Bank of Thailand in March 2025, with implementation from April 2025. These guidelines mandate financial institutions to adopt end-to-end fraud management, strengthen KYC/CDD processes, and enhance support for scam victims[15].
- Enactment of the **Emergency Decree on Technology Crimes (No. 2)** in April 2025, establishing shared liability across banks, telecoms, and platforms, and mandating real-time fraud detection and account suspension. The decree also created the Anti-Tech Crime Center (AMTO) to coordinate enforcement[16].
- Release of the **AI Risk Management Guidelines** in June 2025, establishing governance and lifecycle controls for AI in financial services, and promoting FEAT principles—Fairness, Ethics, Accountability, and Transparency[17].
- Launch of the International **Anti-Scam Coordination Centre (IAC War Room)** in August 2025, a cross-sector enforcement hub led by the Royal Thai Police, Bank of Thailand, SEC, NBTC, and digital platforms, which has significantly improved scam fund interception capabilities[18].

[11] MDES announcement on Anti-Call Center Scam Centre: https://www.mdes.go.th/view/387416

[12] Thailand Digital Government Development Agency (DGA) – Digital ID Framework: https://www.dga.or.th/th/news/2024-digital-id-phase2

[13] Ministry of Digital Economy and Society, Concept note: https://www.mdes.go.th/view/387890

[14] Thailand National Cyber Security Agency (NCSA) – Notifications under Cybersecurity Act: https://www.ncsa.or.th/news/cybersecurity-act-notifications-2025

[15] Bank of Thailand, Consultation paper: https://www.bot.or.th/Thai/FinancialInstitutions/PublicConsultation/Pages/Digital-Fraud-Guidelines-2025.aspx

[16] Ministry of Digital Economy and Society, Draft decree – MDES legal archive: https://www.mdes.go.th/laws/emergency-decree-technology-crimes-no2-2025

[17] Bank of Thailand, AI Risk Guidelines: **https://www.bot.or.th/Thai/FinancialInstitutions/Guidelines/Pages/AI-Risk-Management-2025.aspx**

[18] Royal Thai Police, Cybercrime division press brief: **https://www.tcsc.police.go.th/news/iac-war-room-2025**

Navigating Tomorrow: Enabling Trust, Driving Success

Visa Security Roadmap 2025–2028

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 2025 and beyond.

1. Strengthening cybersecurity to anticipate emerging threats and regulatory shifts
2. Advancing authentication for a seamless experience
3. Enabling safer transactions with tokenised payments
4. Transforming ecommerce checkout to enhance consumer confidence and ease
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 and regulatory shifts

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

From July to December 2024, the number of tracked ransomware and data breach incidents rose sharply to 2,144, representing a 51% increase over the previous six-month period[19]. Threat actors demonstrated greater sophistication and targeted impact, with a continued focus on third-party service providers and file transfer vulnerabilities.

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.

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 cardholder 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.

[19] Visa, Biannual Threats Report, October 2025, https://corporate.visa.com/en/sites/visa-perspectives/security-trust.html

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.

DURING 2022–24,

millions of Thais

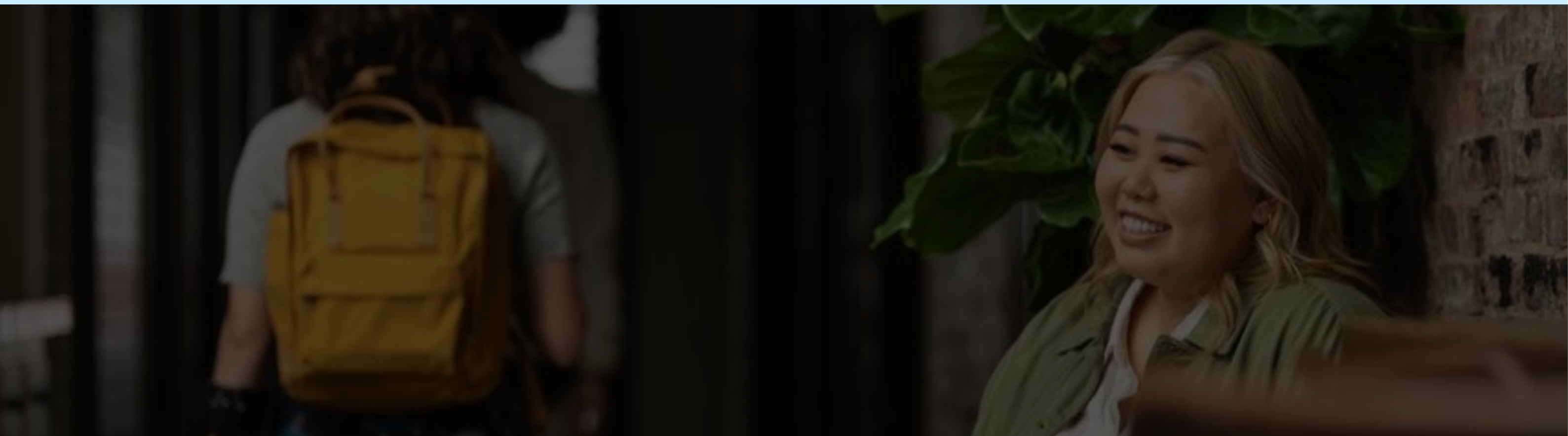
had their private information compromised through significant data breaches,

and some Thais were exposed to multiple breaches[20].

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 Visa[21].

Visa's **Account Information Security Program (AIS)** is a global compliance program dedicated to maintaining the safety and integrity of the Visa payment ecosystem[22]. This is achieved through monitoring compliance and addressing security deficiencies to prevent compromise of Visa account data. As mentioned previously, Visa is transitioning to a more streamlined merchant PCI DSS compliance reporting approach. The 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.

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.



[20] ThaiCERT – National Cyber Security Agency (NCSA), Thailand, หน้าแรก - National Computer Emergency Response Team (NCERT)

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

[22] Visa, Account Information Security Program and PCI, accessed 1 December 2024, https://corporate.visa.com/en/resources/security-compliance.html#:~:text=Visa's%20Account%20Information%20Security%20(AIS,system%20and%20address%20security%20deficiencies.

2

Advancing authentication for a seamless experience

Authentication (EMV® 3DS) continues to play a critical role in Thailand'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 Thailand's push for secure, low-friction digital payments.

However, as phishing and social engineering scams escalate across the Thai 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 some regions have mandated the removal of SMS OTP, encouraging issuers to adopt methods less prone to social engineering[23].

To address the threats of social engineering and strike a balance with a risk-based approach, Visa is recommending issuers to move away from using SMS OTP as the sole factor for authentication by 2028.

Issuers are encouraged to migrate towards more secure authentication methods, such as biometric or in-app authentication, or newer methods like passkeys, app-to-app and app-to-web, which involve multi-channels and/or devices providing higher confidence in the identification process.

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[24]. 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. Another instance is using passkeys. **Passkeys** are a secure and convenient authentication method that uses biometrics or device-based cryptographic keys to replace traditional passwords which are often vulnerable to phishing.

[23] Monetary Authority of Singapore (MAS) has required banks to phase out SMS OTPs as a sole factor to authenticate high-risk transactions, July 2023, https://www.mas.gov.sg/news/parliamentary-replies/2023/written-reply-toparliamentary-question-on-sms-otp-diversions-and-unauthorised-transactions

[24] Visa, Payer Authentication Data Fields in Relation to Visa Secure Program Guide Updates, 17 September 2024, https://support.visaacceptance.com/knowledgebase/knowledgearticle/?code=KA-04583

3

Enabling safer transactions with tokenised payments

As of December 2024, Visa has issued

1.9Billion

tokens in the Asia Pacific region

boosting digital payments while enhancing security[25].

↑ **4.7%** **Authorisation Rate Lift[25]** Global Average for Visa Token CNP transactions

↓ **34%** **Fraud Reduction** Visa Token vs PAN-based CNP transactions[26]

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.

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**[27].

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. **Available in Thailand since October 2023**, VPI is designed to help reduce overall ecosystem fraud and increase the number of valid token provisioning requests.

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

[26] 2 Visa Risk Datamart, Global, FY24 Q1-Q4 Token Fraud Rate vs PAN Fraud Rate by PV. Merchant's individual rates may vary

4

Transforming eCommerce checkout to enhance consumer confidence and ease

Digital payments are transforming how Thais shop and transact—and Visa is leading that change.

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 **Click to Pay (CTP)**. By addressing challenges like cart abandonment, security concerns, and removing friction from the online check out experience, CTP optimises the payment process by eliminating the need for passwords, manual card entry, tedious form fills and various step ups. Instead of relying on traditional Primary Account Number (PAN) entry, CTP uses tokenisation, enhancing both security and convenience for consumers and merchants alike. With CTP consumers can access all their payment cards by entering their phone number or email address, then selecting their preferred card for payment. This consistent experience works across devices, allowing users to complete transactions securely with a few clicks. For merchants, it ensures authenticated payment credentials without requiring consumers to input PANs or passwords.

Built on EMV Secure Remote Commerce standards, the CTP standards are compatible with technologies that enable cardholder verification and tokenisation.

With CTP

consumers use a single profile, across multiple devices and merchants

for cards from participating networks, leveraging existing secure technology standards to reduce friction and improve overall shopping experience.

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

Globally, Visa has also announced the introduction of **Visa Flex Credential**, which seeks to revolutionise the payment experience for cardholders. This new solution allows cardholders to toggle between payment methods via just one single payment credential. Cardholders will have the flexibility to select from their preferred methods and set predefined preferences for each transaction.

With over six billion near field communication (NFC) enabled mobile devices worldwide, contactless payments continue to surge[27]. **Tap to Pay** adoption has doubled since 2019, reaching 65% globally, and Visa is building on this momentum with **Tap to Everything** features. These include **Tap to Accept**, enabling banking apps to turn smartphones into secure acceptance points for small merchants; **Tap to Confirm** for frictionless online shopping; and **Tap to Add Card** for enhanced card security. Each tap transaction is protected by EMV chip technology and dynamic encryption, generating a unique one-time code to prevent counterfeit fraud.

Visa is also expanding **Scan to Pay** for QR-based transactions, catering to Thailand's mobile-first consumers and supporting small businesses with fast, secure, and low-cost acceptance solutions. Together, these innovations deliver speed, security, and simplicity—driving growth and confidence across Thailand's digital commerce landscape.

[27] Visa Reinvents the Card, Unveils New Products for Digital Age, May 2024 https://usa.visa.com/about-visa/newsroom/press-releases.releaseId.20686.html#:~:text=Today%20at%20the%20annual%20Visa%20Payments

5

Leveraging foundational standards to drive network performance

Strengthening the Payment Ecosystem Through Unified Risk and Security Programs.

Visa continues to enhance the integrity, security, and efficiency of the global payment system through a coordinated set of programs 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 programs and updates form the foundation of this effort:

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[28].

Apr'24 ✓ The streamlined **merchant** Payment Card Industry Data Security Standard **(PCI DSS) requirements**[29].

Aug'24 ✓ **Visa Secure** now requires key data elements to help issuers decide whether to approve or challenge transactions with minimal friction[30].

Oct'24 ✓ Updated **Visa Acceptance Risk Standards (VARS)** to help acquirers strengthen security, streamline operations, and collaborate more effectively[31].

Fraud Reporting and Control Program (FRECOP) 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

[28] Visa, Why tokens hold the key to the future: de-risking the evolving payments ecosystem, October 2023, https://navigate.visa.com/cemea/trust-and-security/why-tokens-hold-the-key-to-the-future-de-risking-the-evolving-payments-ecosystem/

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

[30] Visa, Visa Payer Authentication Data Fields in Relation to Visa Secure Program Guide Updates, 17 September 2024, https://support.visaacceptance.com/knowledgebase/knowledgearticle/?code=KA-04583

[31] Visa, Visa Acceptance Risk Standards, 1 October 2024, https://usa.visa.com/dam/VCOM/download/merchants/visa-global-acquirer-risk-standards.pdf

Improving Issuer Fraud Controls

Fraud Reporting and Control Program (FRECOP)

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

Fraud reporting is essential for controlling fraud, mitigating risks across the ecosystem, enhancing payment security and meeting regulatory expectations regarding fraud mitigation. Through accurate fraud reporting, financial institutions and merchants receive actionable insights to optimise their payments and deliver a secure customer experience.

Launching the enhanced Visa Acquiring Risk Compliance Programs

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)[32].

VAMP has the potential to address

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

compared to previous programs 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 program** 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), 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 program 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.

[32] Visa, Introducing the Visa Acquirer Monitoring Program, 30 August 2024, https://usa.visa.com/visa-everywhere/blog/bdp/2024/08/29/introducing-the-visa-1724958906425.html

6

Building a resilient payments ecosystem to combat unauthorised fraud and authorised payment scams

Generative AI is growing fast and becoming more widely used, especially as Thailand'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 Thai consumers and businesses.

In Thailand, 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.

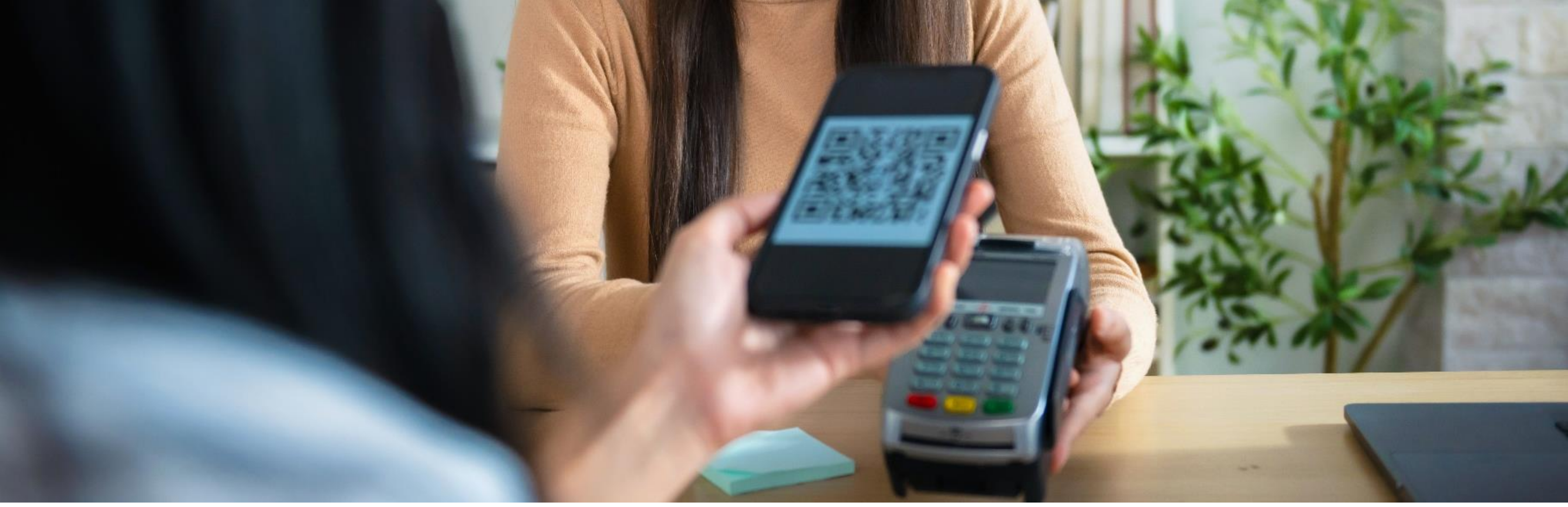
Visa has been using AI in payments for over 30 years. In fact, we were the first network to use AI for real-time fraud detection back in 1993[33]. Today, we run around 150 AI and machine learning models that support products designed to solve problems for consumers, merchants, and financial institutions.

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 Thailand's digital economy.

Looking ahead, Visa Thailand 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 Thailand

[33] 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 Thailand, 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

Issuing fraud rate increased rose significantly YoY, highlighting urgent need for stronger controls.

↑ **30%** YoY in 2024[34]

Key Mer[20]chant 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; **low tokenisation** still leaves issuers exposed.

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

Physical Card Theft: Risk persists where **chip + signature** remains. Moving to **chip + PIN** can strengthen security and protect consumers.

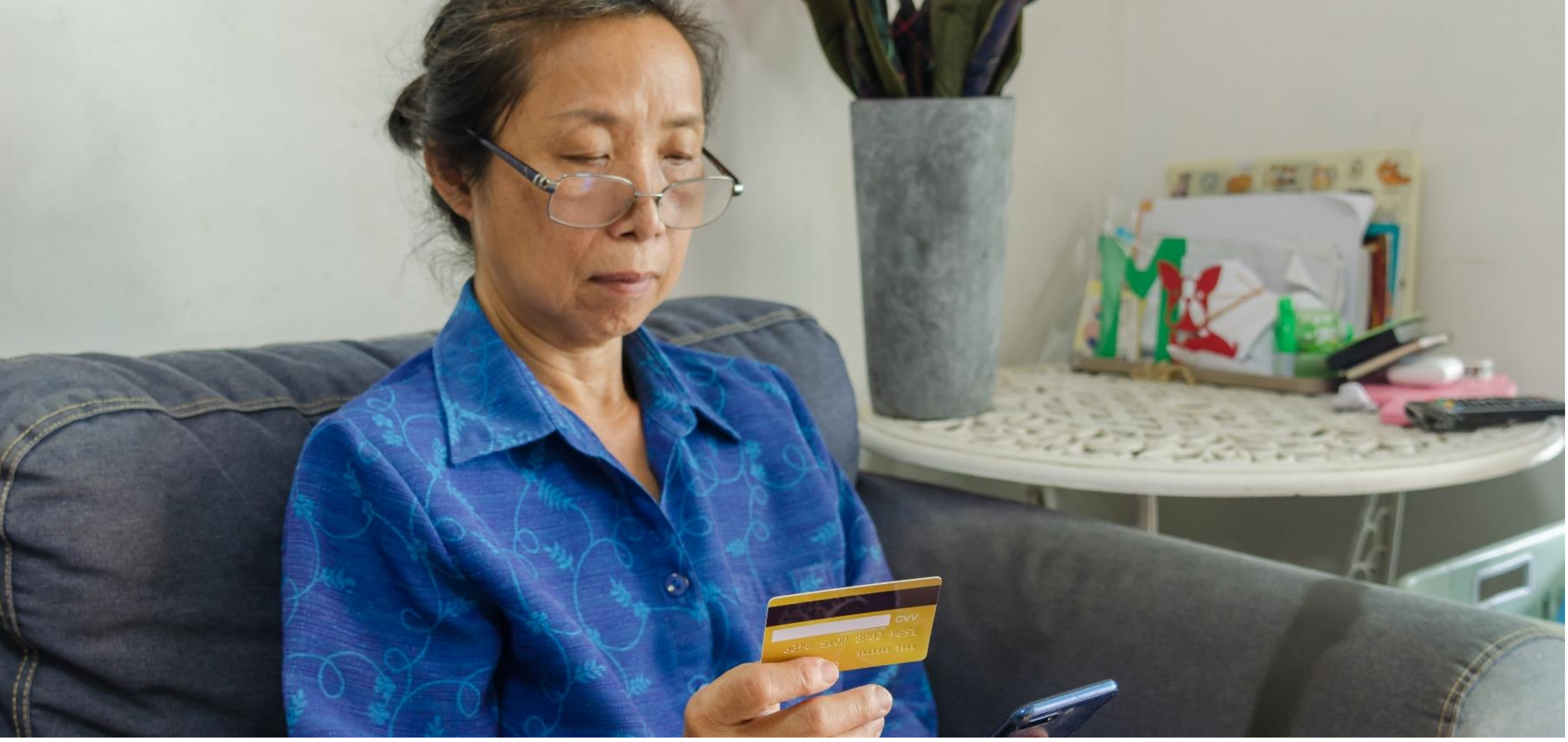
Acquiring fraud

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 defenses 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.

[34] VisaNet, 12 months data ending December 2024, January 2018 to December 2024



Authorised payment (scams)

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

SCAM LOSSES IN THAILAND

2022 **THB 75B**[35]

2023 **THB 98B**[36] ↑ 31% YoY

2024 **THB 115.3B**[37] ↑ 18% YoY

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 Acquirer 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 Thailand.

Visa's expansion into **Real-Time Payments (RTP)** brings its advanced fraud tools—like **Visa Protect for Account to Account (VPAA)** and **Visa Advanced Authorisation (VAA)** 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.

THAILAND SCAM LANDSCAPE: 2024 SNAPSHOT

Highest loss by scam type

- **Investment Scams** 66% of victims lost money
- **Shopping Scams**
- **Employment Scams**

Recovery Rate Only **29%** of victims recovered any funds.

[35] Gogolook, 2022 Annual Fraud Report : Calls and Messages, 15 February 2023, https://www.gogolook.com/newsroom/gogolook-2022-annual-fraud-report-calls-and-messages

[36] GASA, Gogolook, 2023 Asia Scam Report, 14 April 2024, https://www.gogolook.com/newsroom/gogolook-joins-the-global-anti-scam-alliance-gasa-to-become-a-leader-in-the-asian-anti-scam-movement

[37] Global Anti-Scam Alliance (GASA), Thailand Faces Unprecedented Scam Crisis with ฿115.3 Billion Lost Annually, 5 August 2025, Thailand Faces ฿115.3B Scam Crisis – GASA 2025 Report

Visa has actively participated in the creation of different initiatives and tools, contributing to a safer digital environment in Thailand. We continue to put our technology and expertise to work to enhance security, reduce fraud, and deliver seamless digital experiences for Thai consumers and merchants. In addition, Visa has invested over US$10 billion into technology and innovation in the last five years, 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 Protect Authentication Intelligence (VPAI), which leverages data analytics to optimise authentication processes, reducing friction for legitimate users while enhancing fraud detection; and
- 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

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 Thailand 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, driving security alongside payment innovation as we enable new and exciting ways to pay.

Considering these expectations of the Thailand threat landscape in the coming years, Visa has mapped the steps we are already taking with ecosystem partners during 2025 and into the coming three years to highlight the critical areas for action.

2018

- 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
- Block large-scale attacks with Visa Network Defense
- Monitor fraud performance and reporting accuracy with VAMP and FRECOP
- Strengthen merchant onboarding with updated Visa Acceptance Risk Standards (VARS) to block bad actors
- Protect Consumers with Visa's Scam Mitigation Framework

2026-2028

- Conduct annual cyber posture assessments to ensure readiness
- Shift from SMS OTP to biometric / in-app authentication and Visa Payment Passkeys for faster, safer identity verification
- 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 Thailand'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

- ✓ Advance **tokenisation standards** and PDPA alignment to build consumer trust.
- ✓ 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, biometrics, and frictionless authentication—to increase approval rates and reduce fraud.
- ✓ Deliver seamless onboarding and robust dispute management to build consumer trust and operational excellence.

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

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