VISA

The Anti-Scam Playbook: Market Responses and Industry Insights

May 2025

What's Inside

© 2025 Visa. All rights reserved.

Disclaimer

In this document, case studies, statistics, research, summaries 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. You should consult with your legal counsel to determine what laws and regulations may apply to your circumstances. The actual costs, savings and benefits of any observations, recommendations or programs may vary based upon your specific business needs and program requirements. By their nature, recommendations are not guarantees of future performance or results and are subject to risks, uncertainties and assumptions that are difficult to predict or quantify. Visa is not responsible for your use of the information contained herein ("Information") (including errors, omissions, inaccuracy or non-timeliness of any kind) or any assumptions or conclusions you might draw from its use. Visa makes no warranty, express or implied, and explicitly disclaims the warranties of merchantability and fitness for a particular purpose, any warranty of non-infringement of any third party's intellectual property rights. To the extent permitted by applicable law, Visa shall not be liable to you or any third party for any damages under any theory of law, including, without limitation, any special, consequential, incidental or punitive damages, nor any damages for loss of business profits, business interruption, loss of business information, or other monetary loss, even if advised of the possibility of such damages.

Forward Looking Statements

The Information in this document contains forward-looking statements within the meaning of the U.S. Private Securities Litigation Reform Act of 1995. Forward-looking statements generally are identified by words such as "believes", "estimates", "expects ", "intends", "may", "projects", "outlook", "could", "should", "will", "continue" and other similar expressions. Examples of forward-looking statements include, but are not limited to, statements we make about developments in relation to scams in the financial sector and the prevention of scams. By their nature, forward-looking statements: (i) speak only as of the date they are made; (ii) are not statements of historical fact or guarantees of future performance; and (iii) are subject to risks, uncertainties, assumptions or changes in circumstances that are difficult to predict or quantify. Therefore, actual results could differ materially and adversely from our forward-looking statements due to a variety of factors, such as those more fully described in Visa's filings with the U.S. Securities and Exchange Commission. You should not place undue reliance on such statements. Except as required by law, we do not intend to update or revise any forward–looking statements as a result of new information, future developments or otherwise.

© 2025 Visa. All rights reserved.

Executive Summary

Scams are borderless and widespread, affecting individuals and businesses globally. In recent years, the frequency and losses associated with scams have surged, becoming more sophisticated and convincing, especially with the use of Artificial Intelligence (AI).

According to the Global Anti-Scam Alliance (GASA), over US$1 trillion has been lost to scams, between August 2022 and August 2023[1]. Markets in Asia reportedly lost a higher share of their Gross Domestic Product (GDP) to scams compared to the other regions.

Various stakeholders in the ecosystem - including financial institutions, infrastructure providers, social media platforms, payment networks, regulatory bodies, and consumers - play critical roles in combatting scams. Each has specific responsibilities that are vital to building a resilient defence against these threats. Regulators have established anti-scam frameworks to address liability and accountability, and to protect consumers. Across the Asia Pacific region, various anti-scam initiatives focus on authentication, intelligence sharing and raising consumer awareness. The importance of educating consumers about the risks and signs of scams cannot be overstated – a vigilant population remains our first line of defence against scams. With the advancements in AI, agent-led commerce is becoming a reality today. Agentic AI is poised to set a new standard for scaling anti-scam efforts through adaptive anomaly detection and proactive threat prediction.

Visa is committed to partnering with various ecosystem stakeholders to protect consumers and businesses from scams. Over the past five years, Visa has invested over US$12 billion in technology to reduce fraud and enhance network security. Ultimately, a whole-of-ecosystem approach is essential to effectively combat scams and ensure the protection of all parties involved.

> Scams are a borderless threat. Visa is committed to partnering with ecosystem stakeholders worldwide to effectively and efficiently counter scams. Our insights show that an integrated response to scams is essential to safeguarding the ecosystem and ensuring that commerce can continue to thrive in a secure environment.

Stefaan D'Hoore
Regional Risk Officer, Asia Pacific, Visa

[1] Global Anti-Scam Alliance. (2024). Global state of scams report: $1 trillion stolen in 12 months.

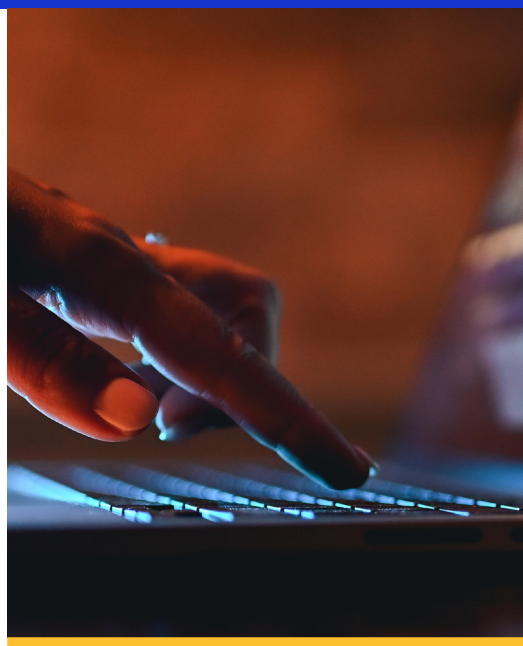
© 2025 Visa. All rights reserved.

Introduction

With the increased adoption and evolution of digital apps and tools, consumers can transfer money seamlessly and quickly. Globally, the digital wallet population is expected to exceed 5.2 billion[2] by 2026, while global retail eCommerce sales are forecast to reach US$6.8 trillion[3] by 2028. However, this has also led to increased opportunities for scammers to deceive consumers and businesses of their money. Globally, scams have been a perennial problem affecting people from all walks of life, with an estimated annual loss of US$1 trillion[4] loss (more than 1% global Gross Domestic Product). This situation is further perpetuated with the use of Artificial Intelligence (AI), making scams more convincing even to discerning people.

Asia Pacific has not been spared from scams. In fact, it is estimated that individual consumers across the region collectively lost US$688 billion[5] to scams in 2024. Specifically, in Singapore, losses arising from scams rose by 145% from S$266 million[6] in 2020 to S$1.1 billion in 2024[7]. In Australia, over A$2 billion[8] was lost in reported scams in 2024, marking a 135% increase from the A$0.85 billion reported loss in 2020. Of note, Taiwanese consumers experienced scam losses of US$7.4 billion[9] in a year, which represents 1% of Taiwan's Gross Domestic Product[10]. As a leading payments provider in the commerce and payments ecosystem, we are committed to bringing more attention to this critical issue in combatting the alarming rates of increase in scam losses.

This white paper examines the anti-scam responses from governments and industry players through three dimensions: the key players involved, the concepts of liability and accountability, and the actions stakeholders across Asia Pacific are taking to combat scams. These perspectives allow us to illustrate how an integrated response can counter scams effectively and efficiently, and ultimately enable all of us to better protect the ecosystem so that commerce can continue to flourish in a safe and secure environment.



Did you know?

US$75 billion

was moved by scammers on crypto platforms between 2021 to 2023[11]

Almost half of the world experiences a scam attempt at least once weekly.

Source: Global Anti-Scam Alliance (GASA) and Feedzai 2024 Global State of Scams Report

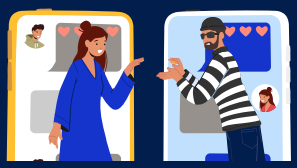
[2] Juniper Research. (2023). Digital wallet users exceed 5.2 billion globally by 2026.
[3] eMarketer. (2023). Worldwide retail eCommerce forecast 2025.
[4] United Nations Development Programme (UNDP). (2023). UNDP launches anti-scam handbook with global coalition partner.
[5] Global Anti-Scam Alliance. (2024). 2024 Asia scam report: $688 billion lost.
[6] Singapore Police Force (2024). Annual Scams and Cybercrime Brief 2023.
[7] Singapore Police Force. (2024, February). Five things you should know about the annual scams and cybercrime brief 2024.
[8] Australian Competition and Consumer Commission. (2024). Targeting Scams Report.
[9] Global Anti-Scam Alliance. (2023). Where Did the Billions Go in Malaysia, Thailand, and Taiwan?
[10] BERNAMA. (2023). News Report.
[11] Griffin, J. M., & Mei, K. (2024). How Do Crypto Flows Finance Slavery? The Economics of Pig Butchering. SSRN.

© 2025 Visa. All rights reserved.

Scams Defined

Often, people assume that fraud and scam mean the same thing. However, there is a subtle difference between these two terms. Scams often involve deceptive practices where the consumer is misled into making a transaction, while fraud can occur without the consumer's knowledge or involvement. Visa defines scam activity as a payment that a cardholder was deceived into making and authorising. This differs slightly from fraud, which broadly involves any unauthorised access to personal information or funds. Scams are borderless and exploit multiple channels, shifting between account-to-account (A2A) transactions and card payments.

Common types of scams[12]



Pig butchering scam

Named after the practice of farmers (scammers) fattening hogs (victims) before slaughter, this scam first involves befriending victims via social media or dating apps. They then build trust with their victims before luring them to either transfer cash or invest in cryptocurrency or other forms of assets through fraudulent platforms.

Law enforcement / bank official impersonation

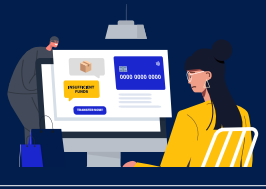
Fraudsters impersonate government officials and convince victims that they are investigated for criminal activities. Victims would be asked not to contact other people, as they are under scrutiny, and the call may be transferred to different parties to add credibility. They would then be asked to transfer money from their accounts for the investigation.

Job scams

Victims are offered to perform tasks remotely to obtain "rewards". Victims may have to pay a certain fee in order to access the higher level jobs. Initially, the scammers would pay out a small commission to buy the trust of victims. Once trust is established, the scammer entices the victim to put in more money. When the victim realises the money cannot be withdrawn, the scammer becomes uncontactable.

ECommerce scams

Victims engage online advertisements on social media platforms or listings on online marketplaces to purchase items and the sellers remain uncontactable after receiving the money. Often, prices of the items are low to entice victims.

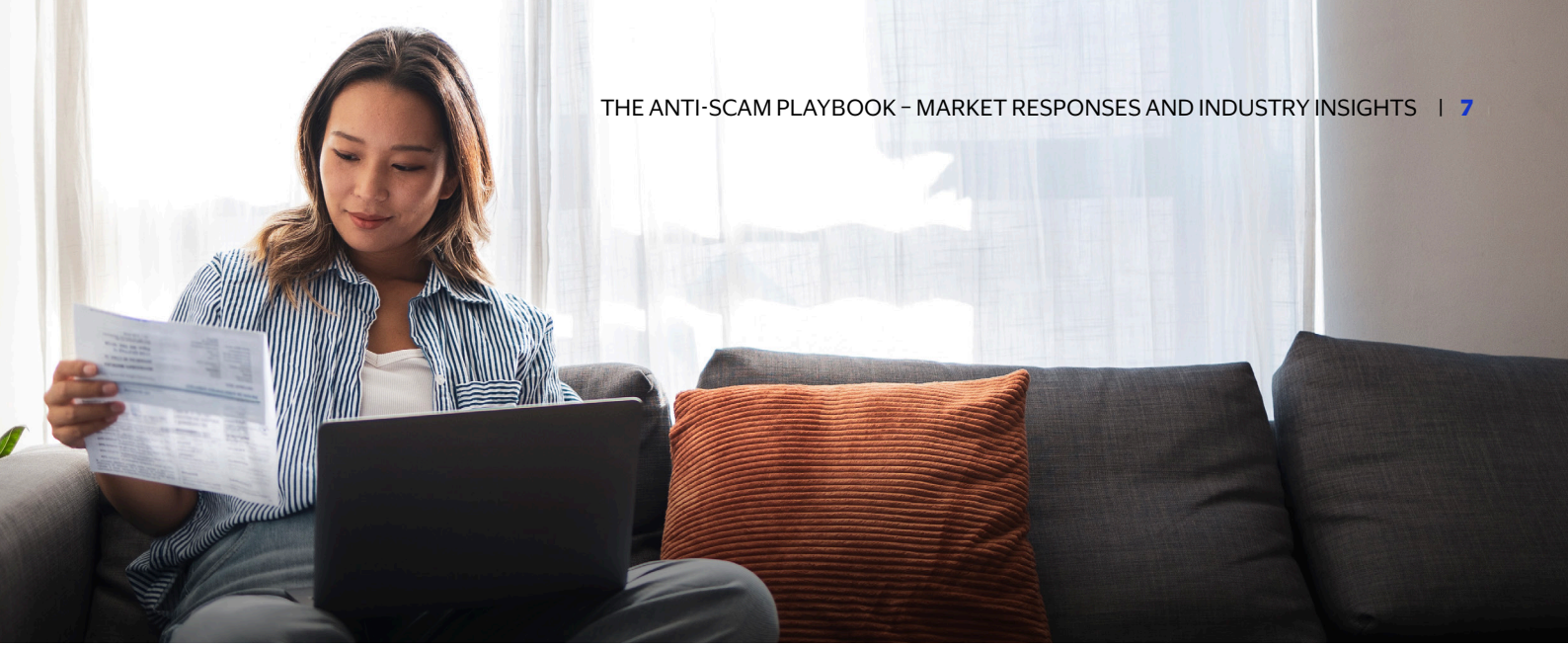


Parcel delivery scams

Victims are informed via text or email that their parcels cannot be delivered due to reasons such as insufficient postage. They will then be re-directed to a link to make the necessary payment, which provide scammers with their personal details.

[12] United Nations Office on Drugs and Crime (October 2024). Transnational Organised Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape.

© 2025 Visa. All rights reserved.

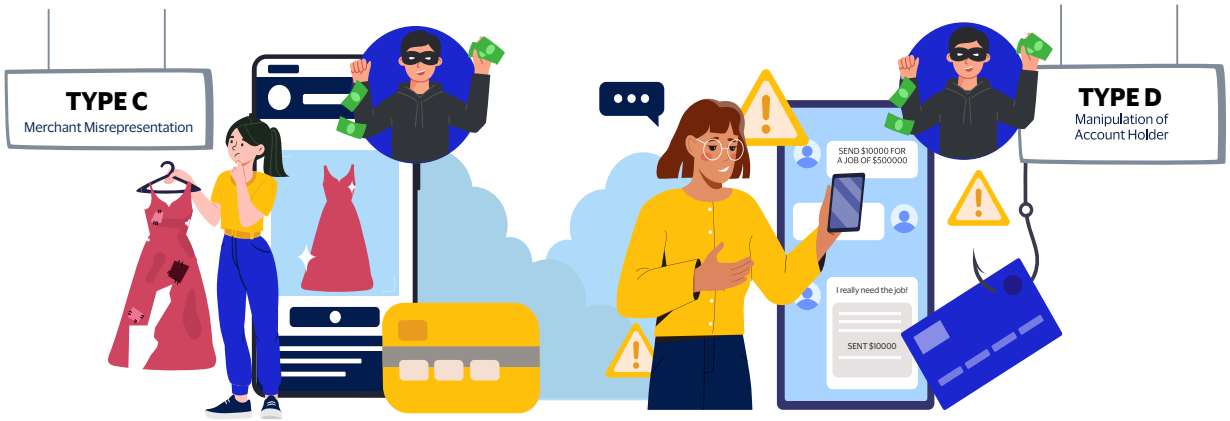


Scams Defined

Currently, there is no common, universally accepted taxonomy for scams. This poses several challenges, including:

- Defining and measuring the full scope of scams, for identification and reporting purposes.
- Facilitating effective communication, data-sharing, and coordinated responses among law enforcement, financial institutions, and other stakeholders.
- Deterring consumers from reporting scams if they are unsure whether they have been scammed or feel responsible for falling victim.

The United States Federal Reserve has developed the ScamClassifier Model[13] to support consistent and detailed classification, reporting, analysis and identification of scams. This model uses a series of questions to classify scams by categories and types. It can capture the full impact of scams by including both cases of authorised and unauthorised payments, as well as attempted scams.



In the context of scams occurring in the Visa network, Visa has taken steps to identify them through identification codes C (Merchant Misrepresentation) and D (Manipulation of Account Holder). Type C is when a merchant deliberately misleads the account holder, such as selling items that are not as they seem. Type D is when a merchant manipulates an account holder into completing what they believe to be a legitimate transaction. This includes the account holder sending funds to a fraudulent beneficiary, falsely believing they will gain fictitious riches or help an individual in distress. Additionally, reporting can be further classified into seven areas, providing more granularity on the type of scam (purchase, investment, romance, advance fee, invoice, CEO fraud, impersonation).

Standardising scam definitions can set the foundation for improving scam detection and prevention efforts. Nevertheless, the ecosystem would need to maintain a balance between detailed classification and adaptability for evolving scam tactics.[14]

[13] Federal Reserve Financial Services. (2024). ScamClassifier Model.
[14] Global Anti-Scam Alliance. (2024). Scam Classification and Measurement: Global Anti-Scam Summit Americas 2024.

© 2025 Visa. All rights reserved.

Who are the Stakeholders Involved in the Anti-Scam Responses?

From the analysis performed, one or more of the following stakeholders (in no particular order) play an active role in the frameworks and approaches established to combat scams.

Financial Institutions

Financial Institutions (FIs), as custodians of consumer funds, play a critical role in scam prevention across various payment channels, including bank transfers, real-time payments, and cards. They are at the forefront of detecting suspicious activity, educating customers, and responding swiftly to reported scams through advanced technology and analytics. Additionally, merchant acquirers must implement stringent due diligence measures during the onboarding process and advanced fraud detection and monitoring tools to prevent fake or collusive merchants from cashing out on fraud.

Cryptocurrency Industry

With the growing adoption of digital assets, the role of the cryptocurrency sector is expanding. Cryptocurrencies are commonly used to perpetuate scams, with scammers moving some US$75 billion in scam proceeds onto cryptocurrency exchanges between 2021 to 2023[15]. To combat scammers exploiting the speed and anonymity of cryptocurrency, exchanges and wallet providers should enhance Know-Your-Client (KYC) and Anti-Money Laundering (AML) practices and implement robust controls on cryptocurrency transfers.

Infrastructure Providers

Telecommunications companies (telcos) provide the infrastructure through which many scams are perpetrated, such as phone calls and text messages, making their cooperation essential in identifying and blocking scam communications.

Technology Platforms

The acceleration of technology and social media allows scams to proliferate quickly, with scammers deceiving users through phishing, fake profiles, and misleading advertisements. Active monitoring, early intervention through scam content detection and removal processes, as well as user education initiatives, are crucial.

Merchants

Merchants, both online and offline, interact directly with consumers and handle transactions daily. They play a vital role in ensuring secure customer journeys, using strong authentication tools, and cooperating with FIs when fraudulent transactions are reported.

Payment Networks

Payment networks play a pivotal role in processing transactions and upholding payments ecosystem security. They work closely with FIs, industry partners and law enforcement to implement measures to detect and mitigate fraud, including by blocking suspicious transaction activity.

Regulatory and Law Enforcement Bodies

Governments and regulators are responsible for setting the policies and frameworks that safeguard against scams, ensuring that there are robust legal and regulatory requirements in place to protect the ecosystem. Law enforcement bodies are responsible for investigating and prosecuting scam activities, ensuring that perpetrators are held accountable. They collaborate with other stakeholders, both domestically and internationally.

Consumers

Ultimately, consumers are at the heart of this ecosystem, serving as both the primary targets of scams and key participants in prevention efforts. Through vigilance and informed decision-making, consumers, as the first line of defence against scams, can protect themselves by staying educated about common scam tactics and reporting suspicious activities.

[15] Griffin, J. M., & Mei, K. (2024). How Do Crypto Flows Finance Slavery? The Economics of Pig Butchering. SSRN.

© 2025 Visa. All rights reserved.

How are Liability and Accountability Addressed in Anti-Scam Frameworks?

Liability and accountability are central to the ongoing debate on how to address scams effectively. In the context of scams, liability refers to the legal obligation to compensate for harm, often requiring responsible entities to reimburse victims for losses incurred. Accountability refers to the duty of these entities to implement effective measures to prevent scams and ensure compliance with regulatory requirements. Regulators design liability frameworks with the goal of consumer protection and seek to attribute scam liability across the different parties involved.

From the analysis performed, different jurisdictions have established regulatory frameworks to address liability and accountability as part of their response to effectively combat scams. This chapter provides a non-exhaustive comparative analysis of the regulatory frameworks developed in the United Kingdom (UK), Singapore, Australia and Taiwan, which were selected for their proactive regulatory measures. As shown in the overview in Appendix 1, each jurisdiction has specific obligations that responsible entities must fulfil to combat scams. Despite variations in scope and applicability, the primary objectives of these frameworks are to address liability, ensure accountability, and protect consumers from scams.

In the UK, the Payment Systems Regulator (PSR) has introduced new rules[16], effective October 2024, whereby victims of Authorised Push Payment (APP) scams will be reimbursed by Payment Service Providers (PSPs) for 100% of losses up to £85,000, unless the victims are found to be 'grossly negligent'.

Key elements include:

- **Liability:** PSPs must reimburse victims up to £85,000 (maximum level). The reimbursement can be split 50:50 between the sending (victim's bank) and receiving (recipient bank used by the fraudster) PSPs.
- **Accountability:** Prescribed timeframes for PSPs in terms of reimbursement windows (within five business days). The sending PSP can pause the five-day timeframe to gather information, but the claim must be concluded within 35 business days from the initial claim.
- **Consumer Protection:** This maximum reimbursement level will mean 99.8% of all Faster Payments APP scams by volume, and 90% by value[17], will be fully reimbursed. The mandatory reimbursement aims to incentivise PSPs to proactively deploy prevention and detection measures to protect consumers from APP fraud. Furthermore, the Payment Services (Amendment) Regulations 2024[18] allow a PSP to delay crediting a transaction to a payee's PSP account in cases of APP fraud.

[16] Payment Systems Regulator. (2024). Groundbreaking new protections for victims of APP scams start today.
[17] Payment Systems Regulator. (2024). APP scams: Maximum level of reimbursement - Policy statement.
[18] The National Archives. (2024). The Consumer Protection (Amendment) Regulations 2024.

© 2025 Visa. All rights reserved.

In Singapore, the Monetary Authority of Singapore (MAS) and Infocomm Media Development Authority (IMDA) introduced the Guidelines on Shared Responsibility Framework (SRF)[19], effective December 2024. This framework clarifies the allocation of responsibility for losses from scams, particularly phishing scams.

Key elements include:

- **Liability:** Cost-sharing is determined via a "waterfall" approach. The responsible FI (which issued the payment account to the consumer) is first in line and expected to compensate the victim for their entire loss if it has breached its obligations. If the responsible FI has fulfilled its obligations but the telco has not, the telco is expected to bear the full loss. If both the responsible FI and telco have fulfilled their obligations, the consumer bears the full loss. MAS' E-payments User Protection Guidelines[20] (EUPG) took effect from December 2024. The EUPG sets out when a consumer can or cannot be held liable for losses arising out of unauthorised transactions. Liability stipulations set out in the SRF and EUPG do not apply to transactions on credit cards, charge cards and debit cards issued in Singapore, which is provided for in the Association of Banks in Singapore (ABS) Code of Practice for Banks – Credit Cards.
- **Accountability:** FIs and telcos must implement anti-scam measures set out in the SRF and EUPG. The EUPG outlines the responsibilities of FIs and consumers in relation to unauthorised and erroneous transactions, and baseline protections FIs should offer to consumers for losses arising from these transactions. The FI duties in the SRF are drawn from the EUPG. Telcos are required to implement authentication measures and anti-scam SMS filters.
- **Consumer Protection:** The SRF and EUPG provide a clear framework for consumer compensation and liability, and a structured process to streamline claims for consumers.

In Australia, the Treasury introduced the Scams Prevention Framework (SPF)[21], effective January 2025. This framework outlines obligations for various sectors.

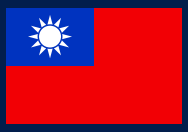
Key elements include:

- **Liability:** Banks, telcos, and digital platform providers are liable if they fail to meet their obligations to prevent scams. The framework allows consumers to seek compensation if these sectors fail to comply with their obligations. The Australian Financial Complaints Authority will decide on the share of compensation for which each sector is responsible.
- **Accountability:** Entities must comply with codes of conduct specific to their sector, which are designed to prevent scams. Detailed obligations are outlined in the Treasury's "Scams - Mandatory Industry Codes"[22] (consultation paper released in November 2023).
- **Consumer Protection:** The SPF sets out the baseline obligations that regulated entities need to fulfil in protecting consumers from scams, through "prevention, detection and disruption".

---

[19] Monetary Authority of Singapore. (2024). Guidelines on shared responsibility framework.
[20] Monetary Authority of Singapore. (2024). E-payments user protection guidelines.
[21] Australian Government Department of the Treasury. (2025). Publication.
[22] Australian Government Department of the Treasury. (2023). Consultation.

© 2025 Visa. All rights reserved.

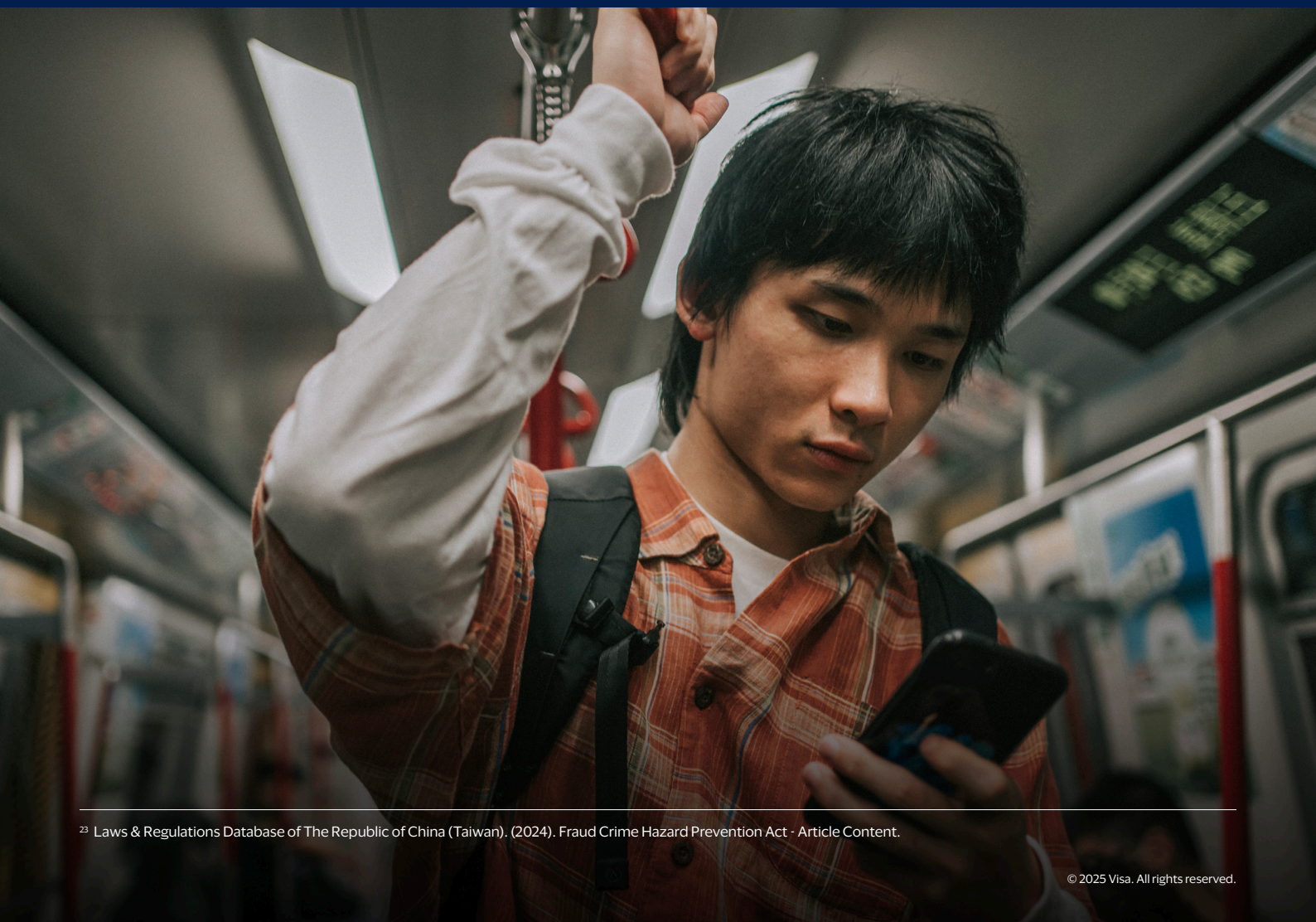


In Taiwan, the Ministry of Interior enacted the Fraud Crime Hazard Prevention Act[23] (FCHPA) in July 2024, in response to intensifying digital financial crime. The law applies to a range of industries, primarily digital platforms that advertise heavily online in Taiwan.

Key elements include:

- **Liability:** Digital platforms and fraudulent advertisers are jointly liable if they fail to meet their obligations.
- **Accountability:** FIs, Virtual Asset Services Providers (VASP), telcos, digital platforms, eCommerce merchants and third-party payment services providers are required to take specific fraud prevention measures, with penalties for non-compliance.
- **Consumer Protection:** The regulations mandate swift action for removing fraudulent advertisements, establish information disclosure and identity verification requirements for advertisers and sponsors, and introduce fraud prevention plan and transparency report obligations. These measures seek to prevent the spread of fraudulent advertisements and increase accountability of advertising platforms in Taiwan.

The regulatory frameworks in the UK, Singapore, Australia and Taiwan represent multi-faceted strategies to address the rising threat of scams. These frameworks set clear expectations for ecosystem stakeholders to enhance their anti-scam measures. Although varying in scope and applicability, all four frameworks aim to clarify liability and accountability, strengthen consumer protection, and establish clear paths for victim recourse. By considering these approaches, other jurisdictions can develop tailored frameworks that bolster resilience against scams, protect consumers, and uphold the integrity of financial systems globally.



[23] Laws & Regulations Database of The Republic of China (Taiwan). (2024). Fraud Crime Hazard Prevention Act - Article Content.

© 2025 Visa. All rights reserved.

How are Stakeholders Responding to Scams?

Having examined the regulatory frameworks established in the UK, Australia, Singapore and Taiwan, it is evident that accountability is imperative to effective scam prevention and mitigation. Underpinning these frameworks are obligations that stakeholders must fulfil to combat scams.

Even in the absence of formalised scam prevention frameworks, regulatory and industry bodies across the Asia Pacific region are actively implementing measures to combat scams. In this chapter, we delve deeper into both formal obligations and industry-led initiatives undertaken by stakeholders, which can be classified into three categories – authentication, intelligence sharing and raising consumer awareness. We explore how these efforts bolster scam prevention efforts and ensure a coordinated response (a non-exhaustive overview is shown in Appendix 2).

Authentication

Authentication methods play a critical role in disrupting scams by ensuring that only authorised individuals can access and execute transactions. Implementing the concept of "smart friction" is essential in this process, as it introduces just enough security measures to verify legitimacy without overly burdening the user.

Secure communication channels

One common method which scammers deploy is to masquerade their SMS sent to mobile users using the same alphanumeric sender identification (Sender ID) used by genuine businesses and organisations. To combat this, in 2022, Singapore's Infocomm Media Development Authority (IMDA) established the Singapore SMS Sender ID Registry (SSIR)[24] – a central body for the registration of Sender IDs to be used in Singapore. An SMS that attempts to spoof the registered Sender IDs will be blocked upfront. A similar registry[25] was launched in Australia in December 2023. In January 2025, the Reserve Bank of India (RBI) published regulations[26] on prevention of financial fraud perpetrated using voice calls and SMS. This requires regulated entities to utilise the Mobile Number Revocation List (MNRL) available on a central Digital Intelligence Platform (DIP) and using specific numbering series for commercial calls, amongst other measures. Sending hyperlinks via SMS from FIs has been banned in Asia Pacific markets such as Singapore[27], Malaysia[28], and more recently Thailand[29] due to the surge in SMS-phishing scams.

Applicability: *Financial Institutions / Telcos / Payment Networks / Merchants*

FI-telco collaboration

Interestingly, there is greater collaboration across various sectors such as FIs and telcos to fight scams through technological innovation. This is partly because these sectors tend to be intertwined in scams, prompting more coordinated responses as a solution. In a news release, Telstra, one of the biggest telcos in Australia, and the Commonwealth Bank of Australia (CBA) announced Scam Indicator[30], their anti-scam collaboration to detect and intercept suspicious calls on mobile phones. It was then expanded to landlines to protect their most vulnerable customers. Another publicised collaboration in Australia involves Westpac and Optus, who worked together to introduce an in-app calling capability for Westpac customers to reduce bank impersonation scams[31]. The solution, which is Westpac-branded and verified by Optus, shows the reason for the call, providing more legitimacy and reducing impersonation risk.

Applicability: *Financial Institutions / Telcos*

[24] Infocomm Media Development Authority. (2022). Full SMS sender ID registration to be required by January 2023.
[25] Australian Communications and Media Authority. (2025). SMS sender ID register.
[26] Reserve Bank of India. (2025). Prevention of financial frauds perpetrated using voice calls and SMS – Regulatory prescriptions and Institutional Safeguards.
[27] Monetary Authority of Singapore. (2022). MAS and ABS announce measures to bolster the security of digital banking.
[28] Bank Negara Malaysia. (2023). Annual Report 2023.
[29] Nation Thailand. (2023). Banking & Finance.
[30] Telstra. (2023). Telstra and CommBank expand collaboration to increase fraud detection rates.
[31] Westpac. (2024). Westpac SafeCall will allow customers to report scams easily.

© 2025 Visa. All rights reserved.

Digital identity

Increasingly, governments are moving towards biometric identification methods as a more secure form of authentication. Since 2018, Singapore has adopted Singpass, a national digital and biometric identification system which allows users to access government data sources, public services and private platforms, including financial services such as setting up bank accounts and mobile phone registration. Beyond the SRF, the MAS and the IMDA are exploring stronger, out-of-band authentication solutions, including Fast IDentity Online (FIDO)-compliant tokens, to enhance defences against unauthorised phishing transactions. The Australian Government has also passed the Digital ID Bill 2024[32] to establish a national digital ID system, which aims to provide secure and convenient ways for individuals to verify their identity online.

Applicability: *Financial Institutions / Technology platforms / Merchants*

Tokenisation

Payment tokens are unique, encrypted digital identifiers that replace card details needed to complete eCommerce transactions, creating security and convenience for consumers. In India, tokenisation-related services operate under the mandate[33] issued by the RBI. The Hong Kong Monetary Authority (HKMA) and the Securities and Futures Commission (SFC) are actively promoting and developing tokenisation and digital assets, with initiatives like Project Ensemble[34] and the Digital Bond Grant Scheme[35], while also issuing guidance on tokenised products and virtual assets. In Taiwan, the Bankers Association outlined a series of self-regulatory guidelines in 2024 regarding device wallet provisioning.

Applicability: *Financial Institutions / Merchants / Regulators / Industry Bodies*

Secure out-of-band authentication

SMS has become a ubiquitous tool for both personal and business interactions and has inadvertently become a medium for scammers to exploit their victims. Authorities in markets such as Hong Kong[36], Singapore[37] and Malaysia[38] have been encouraging the use of out-of-band authentication – where users verify transactions through a separate, secure channel like a mobile app with biometrics, as a safer alternative to SMS one-time-password. If SMS authentication is inevitable (e.g., when a consumer cannot install the app), issuers are advised to tighten monitoring of such transactions.

Applicability: *Financial Institutions*

[32] Parliament of Australia. (2024). Digital ID Bill 2024.
[33] Reserve Bank of India. (2021, February 5). Master Direction – Non-Banking Financial Company – Housing Finance Company (Reserve Bank) Directions, 2021.
[34] Hong Kong Monetary Authority. (2024). HKMA unveils Project Ensemble to support the development of the Hong Kong tokenisation market.
[35] Hong Kong Monetary Authority. (2024). HKMA launches Digital Bond Grant Scheme.
[36] Hong Kong Monetary Authority. (2024). Enhancement measures for online payment card transactions.
[37] Monetary Authority of Singapore. (2024). Banks in Singapore to strengthen resilience against phishing scams.
[38] Ministry of Communications and Multimedia Malaysia. (2024). Financial institutions instructed by Bank Negara to beef up security against financial scams.

© 2025 Visa. All rights reserved.

Intelligence sharing

Information-sharing can significantly enhance the ability of entities to detect and prevent scams. Collective intelligence can help to identify new scam tactics more quickly and enable all participants to take preventive measures. One key global initiative was the establishment of the Global Anti-Scam Alliance . Their key mission is to gather governments, law enforcement groups, and industry partners to exchange information and work together to prevent scams. They created the Global Signal Exchange, which is a platform for sharing real-time insights on scams and fraud abuse data[39].

Data exchanges

Independent data sharing exchanges like the Australian Financial Crimes Exchange (AFCX) provide a platform for entities to share information about potential scams in a secure and efficient manner. In Singapore, ScamShield[41] offers a suite of products and tools, including an app and a website, to help citizens identify and report scams.

Anti-scam centres

Regionally, anti-scam centres have been established in several markets, including Hong Kong (Anti-Deception Coordination Centre), Singapore (Anti-Scam Command), Malaysia (National Scam Response Centre), Australia (National Anti-Scam Centre) and Taiwan (National Police Agency's Anti-Scam Unit) to facilitate collaboration and threat responses between the private sector, regulators, and law enforcers. In May 2024, Singapore and Malaysia worked together to recover fraudulent funds after the victim in Singapore transferred money into a bank account in Malaysia[40].

Industry forums

In addition to formal data sharing exchanges, industry forums and associations play a crucial role in information sharing. These forums provide opportunities for entities across various industries to share insights, discuss emerging trends, and collaborate on solutions. Furthermore, they foster a sense of community and collective responsibility in combatting scams. An example is Australia's Scam Safe Accord[42], developed by the Australian Banking Association (ABA), which outlines measures to disrupt, detect and respond to scam activity.

Applicability: *Financial Institutions / Regulatory and Enforcement Bodies*

[39] Global Anti-Scam Alliance. (2025). Global Signal Exchange.
[40] The Straits Times. (2023). More countries set up anti-scam centres; increased teamwork, speed vital to retrieve lost funds: SPF.
[41] ScamShield. (n.d.). https://www.scamshield.gov.sg/
[42] Australian Banking Association. (2023). Scam-safe accord.

© 2025 Visa. All rights reserved.

Consumer awareness

A discerning and vigilant public remains the first line of defence against scams. Individuals have a direct responsibility to mitigate scams by exercising proper cyber hygiene and discernment over disclosure of personal credentials.

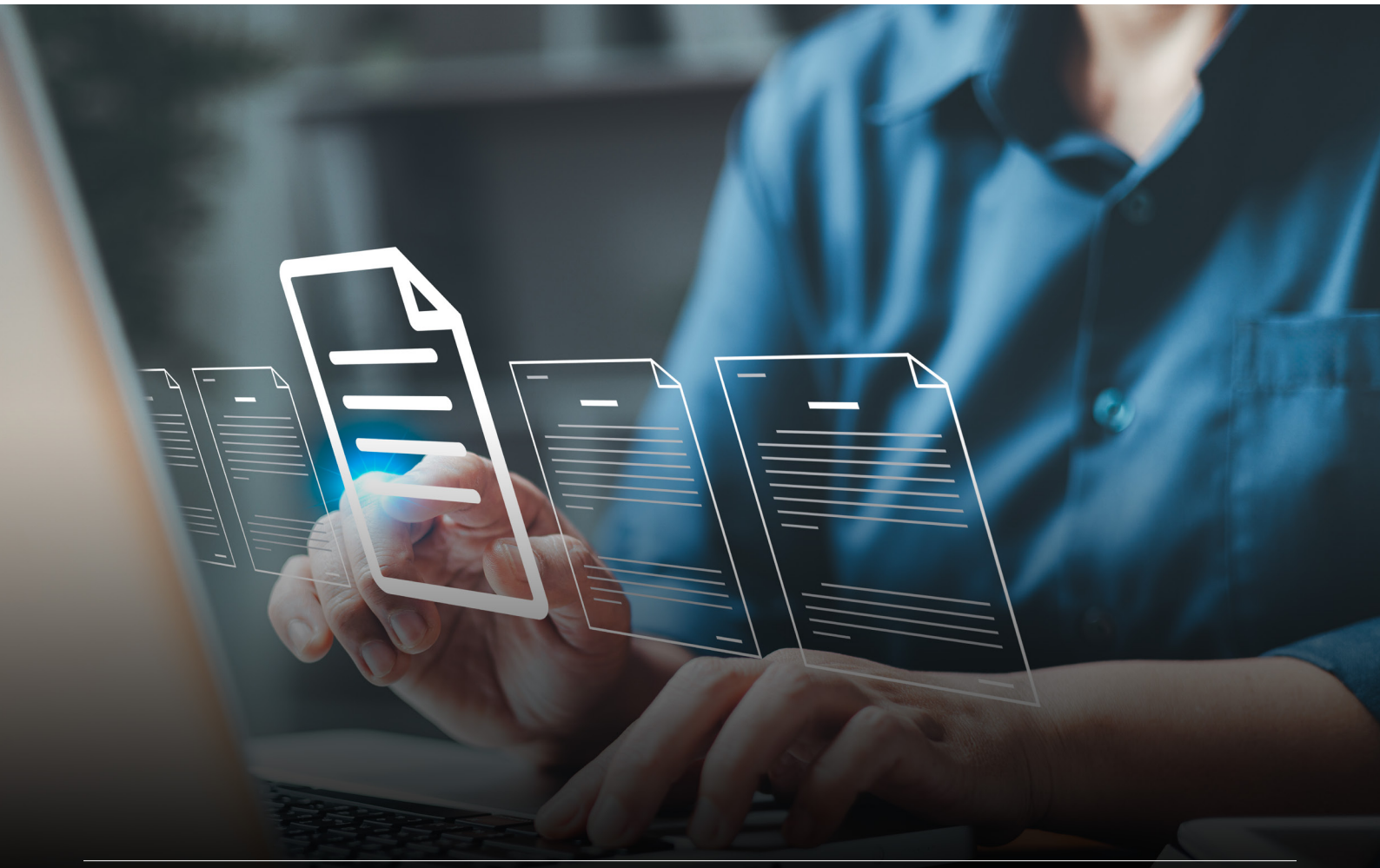
Payment controls

Payment controls to manage card security features are essential measures for fraud detection. The MAS mandates banks to implement transaction alerts and high-risk transaction warnings, including thresholds for notifications, and online transfers, delays for new token activations, and cooling-off periods for key account changes. Similarly, the Australian Scam-Safe Accord recommends deploying card controls, including enhanced warnings, delays, and placing limits on high-risk channels. Card controls are increasingly placed in the hands of consumers, giving them more control over their own security. Complementing these payment controls are requirements for clear messaging in customer notifications.

Public scam search engines

Banks and regulatory bodies have been emphasising consumers' individual responsibility to be vigilant against scams by educating the public on the typologies of scams and how to avoid them. For example, the 'Scameter' was set up by Cyber Defender in Hong Kong to help the public identify frauds and scams. There is also an app, Scameter+, which detects calls and websites on consumers' devices that may be related to scams or frauds[43].

Applicability: *Financial Institutions / Regulatory and Enforcement Bodies*



[43] CyberDefender. (n.d.). Scameter. https://cyberdefender.hk/en-us/scameter/

© 2025 Visa. All rights reserved.

> Fraud usually has no face, but a scam is personal. These scams directly impact the lives of victims, sometimes with devastating effects.

Michael Jabbara
Global Head of Payment Ecosystem Risk and Control, Visa

Initiatives within Visa

Visa believes that a collective industry approach to education and awareness is key to preventing consumers and businesses from becoming victims of scams. Visa works closely with our clients on deploying best-in-class fraud management capabilities and delivering best practices in consumer education and ecosystem awareness to combat fraud and scams. With over 11 billion endpoints and over 200 billion annual transactions across our network, Visa holds uniquely extensive data on scam trends and sources and actively works with law enforcement agencies and industry groups globally on intelligence-sharing. Worldwide, Visa has invested approximately US$12 billion in technology and innovation over the last five years to stop fraudsters and protect merchants and consumers from losses. Specifically, Visa has implemented several strategies and solutions to manage scams:

Visa Scam Disruption Practice

The Visa Scam Disruption (VSD) Practice[44] was unveiled in March 2025 to tackle scams targeting consumers in Visa's ecosystem. VSD aims to protect consumers, clients and businesses by leveraging Visa's deep expertise, technologies, and partnerships:

- **Scam Intelligence:** VSD brings together a cross-disciplinary team that deploys mitigation strategies across various scams. In addition to hiring best-in-class engineers and artificial intelligence developers, Visa has focused recruitment efforts on non-traditional career paths in the fight against scams, looking to former law enforcement, military professionals and data visualisation experts.
- **Proactive Scam Investigations:** VSD mitigates scams through a proactive investigation process that leverages multiple channels and methodologies to identify and address scams before they inflict devastating losses on consumers.
- **Scam Detection and Disruption:** VSD leverages cutting-edge technology and extensive proprietary network-level data to analyse and thwart scams. Investigators use Generative AI tools which enable correlation and graphing analysis to identify complex relationships and parse through mass amounts of data to identify true positive and impactful scam activity. Visa then partners with financial institutions, law enforcement agencies, and third-party partners to disrupt the scam network infrastructure. By collaborating with key stakeholders, VSD aims to dismantle scam operations and prevent future fraudulent activities.

By uncovering the tactics, tools, and infrastructure used by threat actors, VSD can dismantle scam campaigns at their source.

Applicability: *Whole ecosystem*

[44] Visa. (2025, March). Visa unveils its scam disruption practice, helping protect consumers and the financial ecosystem globally.

© 2025 Visa. All rights reserved.

Visa Protect Account-to-Account (VPA2A)

Visa Protect is a suite of risk and identity products designed to safeguard consumers and businesses with new AI-powered solutions for transactions both on and off Visa's network. Scams are more likely to be account-to-account transactions. Under Visa Protect, a solution called Visa Protect for Account-to-Account (VPA2A) was created to provide a real-time risk scoring capability for FIs to make informed decisions about the probability of fraud and scams before funds are sent. This scoring leverages Visa proprietary models, card data, local real-time payments network data and learnings from fraud trends across the globe. For instance, Visa has launched VPA2A in the United Kingdom[45] following a successful pilot where the solution detected 54% of the fraudulent transactions that had passed through the banks' fraud detection systems. In addition, VPA2A was adapted to Argentina's Real Time Payment (RTP) ecosystem and launched in partnership with COELSA, a core payments technology company in Argentina[46].

Applicability: *Issuers*

Fraud Reporting

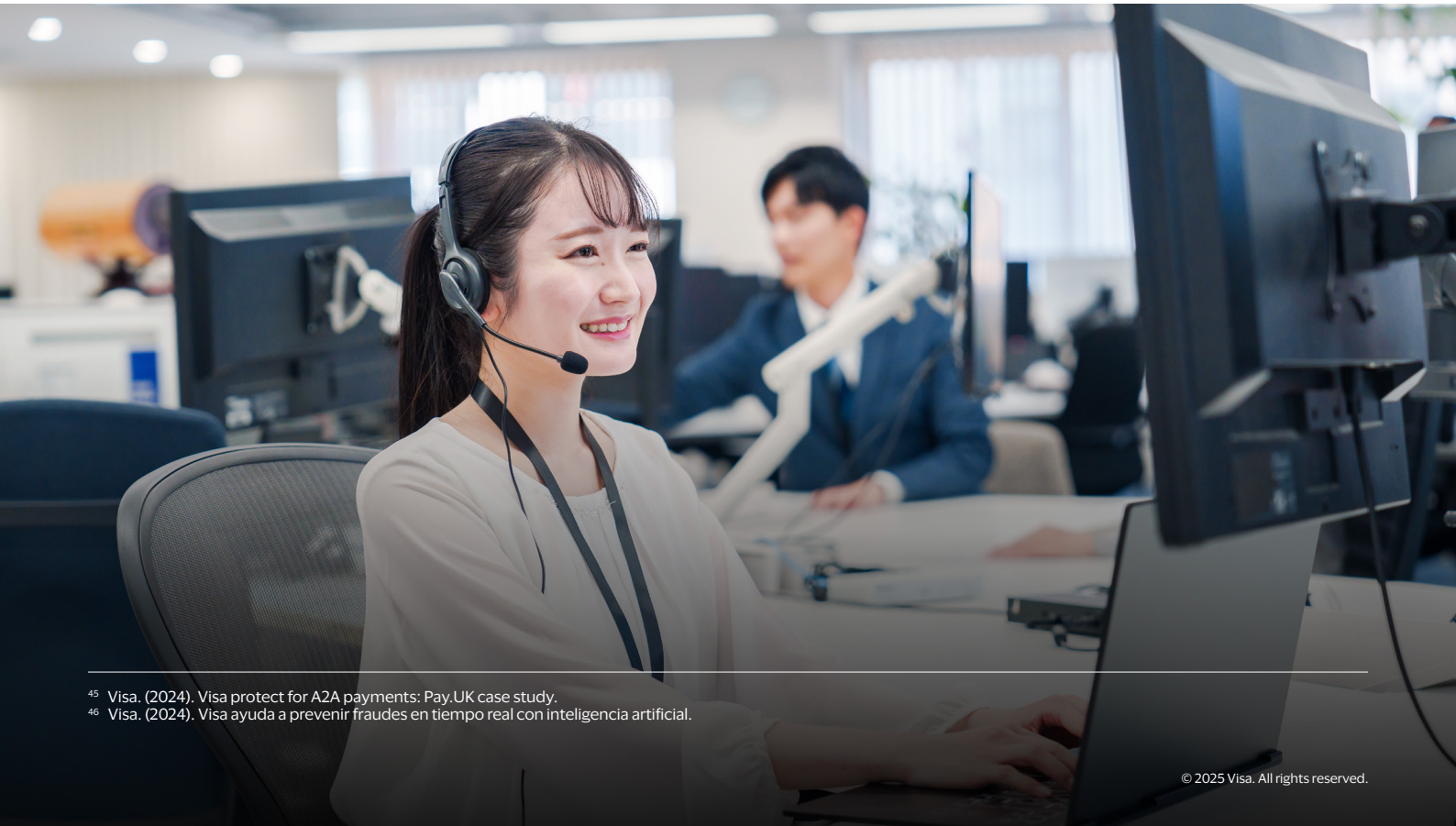
Issuers are required to report and tag scams on Visa rails, which benefits clients in the long run through improved solutioning and intelligence. Visa has introduced more granularity in our fraud reporting mechanisms to enable more detailed reporting of scams, separate from general fraud. This allows for a clearer understanding of different scam tactics. Visa has observed a surge in reported scams in recent quarters (triple digit year-on-year growth). However, we recognise that not all scams are captured in these reports, and there is more to uncover to get a complete picture of the scams landscape.

Applicability: *Issuers / Acquirers / Merchants*

Visa Payment Threat Intelligence

Aiming to provide best-in-class proactive intelligence, Visa Payments Threat Intelligence (VPTI) merges threat intelligence with Visa's network-level data to provide tailored reports and insights on key threats and threat actors targeting a specific industry or organisation. Alerts regarding potential breaches of merchant or customer accounts as well as infrastructure are provided. Additionally, there is a managed service component where a dedicated risk analyst offers clients dark web intelligence specific to their organisation and strategies to strengthen scam prevention.

Applicability: *Issuers / Acquirers / Merchants*



[45] Visa. (2024). Visa protect for A2A payments: Pay.UK case study.
[46] Visa. (2024). Visa ayuda a prevenir fraudes en tiempo real con inteligencia artificial.

© 2025 Visa. All rights reserved.

Tokenisation

Asia Pacific's digital economy experienced an uplift of more than US$2 billion in 2023 [47] as a result of Visa Token Service (VTS) adoption, with token penetration across Asia Pacific approaching a tipping point. VTS replaces the 16-digit debit or credit card number with a unique identifier called 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. Tokens can also improve payment processing by enabling greater control and enriching data exchange for each transaction. These improvements have reduced cases where legitimate transactions are declined by payment systems – an experience that can be frustrating for consumers and merchants. Merchants who have adopted VTS for their digital payments have experienced a higher payment success rate while payment fraud rates are reduced by more than half (58%)[48].

Applicability: *Whole ecosystem*

Visa Rules

Visa's system of rules[49] (The Visa Core Rules and Visa Product and Service Rules or "Visa Rules") allows us to offer consistently safe and reliable access to our network across the globe. The Visa Rules support the use and innovation of Visa products and services and represent a binding contract between Visa and its clients. Designed to minimise risks, these rules are based on global principles while accommodating region-specific and domestic regulations. This allows cardholders, merchants, issuers, and acquirers to transact efficiently and reliably without the need to individually vet one another. Distributed exclusively to clients for managing their Visa programmes, the Visa Rules ensure information parity across the ecosystem. They govern system use and access, setting parameters for participation rights, transaction requirements, risk and security controls, and dispute resolution processes, protecting participants in the network. The Visa Rules provide a high degree of legal certainty between clients regarding their obligations and responsibilities in the system, including those pertaining to settlement procedures, liability, transaction disputes and any events of default.

---

[47] Visa. (2023, October 5). Visa tokens bring USD 2 billion uplift to digital commerce in Asia Pacific. Visa.
[48] Visa Risk Datamart, Global, FY22 Q1–Q4 Token Fraud Rate vs PAN Fraud Rate by PV for merchants with over 1,000 CNP token transactions per month per country. Merchant's individual results may vary.
[49] Visa. (2024). Visa Core Rules and Visa Product and Service Rules.

© 2025 Visa. All rights reserved.

Conclusion

Scams are a pervasive and evolving threat that impacts individuals, businesses, and economies worldwide. The increasing sophistication of scams, particularly with the use of AI, necessitates a whole-of-ecosystem solution.

The insights provided in this whitepaper highlight the critical roles played by various stakeholders, including financial entities, infrastructure providers, social media platforms, payment networks, regulatory and enforcement bodies, and consumers. Each of these stakeholders has specific obligations and responsibilities that are essential for creating a resilient defence against scams.

Anti-scam regulatory frameworks in different jurisdictions, such as the UK, Singapore, Australia and Taiwan, offer valuable lessons in addressing scams effectively. These frameworks emphasise the importance of defining liability and accountability to protect consumers. By learning from these varied approaches, other regions can develop tailored strategies to bolster resilience against scams and protect consumers. Appendices 3 and 4 outline case studies on the scam environment in Singapore and Australia, as well the strategies adopted by these markets, in response to this threat.

Nevertheless, fulfilling these obligations alone is not sufficient to absolve stakeholders of responsibility. A holistic and layered approach that includes collaboration among all players in the ecosystem, continuous improvement of fraud prevention technologies, and active consumer education are crucial to creating a resilient defence against scams.

From authentication and intelligence sharing to regulatory frameworks, there is no single solution for scams. Ultimately, through domestic and international cooperation, stakeholders can minimise the impact of scams on society and ensure a secure environment for all. Visa is committed to assisting the ecosystem in achieving this vision, ensuring robust protection throughout the entire process. Through shared efforts, continuous vigilance, and proactive measures, we can collectively build a stronger, more secure defence against the ever-evolving threat of scams. As we enter the new horizon of agentic commerce, agentic AI is expected to revolutionise fraud prevention by autonomously detecting, responding to, and mitigating fraud threats in real-time, through a network of specialised models. The time is now, for us to be ready for this new agent-led commerce era and, for the ecosystem to get ahead in providing greater trust and security to all.

© 2025 Visa. All rights reserved.

Appendix 1: Anti-Scam Regulatory Frameworks

Aspect	United Kingdom (UK)	Singapore	Australia	Taiwan
Name of framework	Faster Payments Authorised Push Payment (APP) scams reimbursement requirement	Guidelines on Shared Responsibility Framework (SRF)	Scams Prevention Framework (SPF)	Fraud Crime Hazard Prevention Act (FCHPA)
Regulatory Body	Payment Systems Regulator (PSR)	Monetary Authority of Singapore (MAS) and Infocomm Media Development Authority (IMDA)	Treasury, Australia Competition and Consumer Commission (ACCC)	Ministry of the Interior, Financial Supervisory Commission, Ministry of Digital Affairs, National Communications Commission
Effective date	October 2024	December 2024	January 2025	July 2024
Definition of scam	An APP scam involves a victim authorising a payment to an account they believe belongs to a legitimate payee but is actually controlled by a scammer.	A scam involves seemingly authorised transactions where the consumer is deceived into making payments or giving personal information.	An attempt to deceive a consumer into making a payment or giving personal information to a scammer using a regulated service, is considered a scam even if unsuccessful and does not lead to a loss.	Reference to Criminal Code Art. 43, Art. 44 and Art. 339-4
Scope (coverage)	Covers APP scams processed on Faster Payments and Clearing House Automated Payment System (CHAPS).	Covers phishing scams with a digital nexus (i.e., where consumers are deceived into clicking on a phishing link and entering their credentials on a fake digital platform, thereby allowing for unauthorised transactions to be performed from the account) and a Singapore nexus.	All scams falling under the SPF definition. Excludes fraud that involves dishonestly obtaining a benefit without any consumer action, cybercrime, transactions involving faulty products and transactions performed under the threat of imminent violence.	Covers organised scams, impersonation scams and digital scams.
Scope (applicability)	Applies to all Payment Service Providers (PSPs) in the UK, including those using the Faster Payments System (FPS) or CHAPS.	Applies to FIs and telcos in Singapore, covering transactions that seem authorised by consumers.	Initial launch applies to banks, telcos, and digital platforms, with other sectors expected to be added over time.	Applies to FIs, Virtual Asset Services Providers (VASP), telcos, digital platforms, eCommerce merchants, and third-party payment services providers.
Who is liable?	PSPs are liable for reimbursement, unless the consumer was found to be acting with "gross negligence".	FIs and telcos are liable if they fail to meet their obligations under the SRF.	Banks, telcos and digital platform providers are liable if they fail to meet their obligations under the SPF.	Digital platforms and online advertisers will be jointly liable if they do not meet their obligations under the FCHPA.
Cost-sharing element	Reimbursement can be split 50:50 between sending (the victim's bank) and receiving (the recipient bank used by the fraudster) PSPs.	Losses are shared based on whether FIs and telcos have fulfilled their duties ("waterfall" approach). Outlines detailed workflows for reporting authorised transactions and loss-sharing.	Obligations are enforced through civil penalties for non-compliance, and the collaborative approach aims to distribute responsibility across sectors (codes for specific sectors are under review, as at November 2023).	Digital platforms and online advertisers will be jointly liable if they do not meet their obligations. Non-compliant platform operators may also face additional traffic management measures, access restrictions or domain-blocking measures to prevent ongoing harm.
Intelligence sharing	Consumers should, after making a reimbursement claim, and upon request by their PSP, consent to the PSP reporting to the police on the consumer's behalf, or request the consumer directly report the details of an APP scam to a competent national authority.	FIs and telcos are expected to share scam-related information to mitigate risks.	Requires businesses to share actionable scam intelligence with the ACCC, which will be able to distribute it to other businesses, law enforcement and international partners so they can take action to prevent, detect, and disrupt scams.	FIs and VASPs are required to respond to the inquiries of any other FIs and quasi-FIs for the purpose of preventing fraud and scams.
Obligations of stakeholders	- Reimburse victims up to £85,000 (max. level, in line with FSCS) within 5 business days. - No minimum threshold for claims, but there will be a claim excess of £100 at the discretion of the PSP. - Provide clear communication to consumers about risks of APP fraud and their rights under the reimbursement policy.	- FIs and telcos must implement specific safeguards, such as fraud monitoring, real-time alerts, and SMS anti-scam filtering. Detailed obligations of responsible FIs and consumers are set out in the "E-Payments User Protection Guidelines". - Share scam-related information. - Follow operational workflows for reporting scams.	- Comply with sector-specific codes of conduct. Detailed obligations are outlined in the Treasury's "Scams - Mandatory Industry Codes" (under review, as at November 2023) - Businesses that do not meet their obligations under the SPF can face fines of up to A$50 million.	- Mandatory removal of fraudulent ads within 24 hours upon notification from law enforcement - Implement robust identity verification measures - Enhanced information disclosure in ads - Establish and implement a fraud prevention plan and publish an annual fraud prevention report. - Non-compliant FIs and VASPs may be penalised up to NT$2 million.

© 2025 Visa. All rights reserved.

Appendix 2: Anti-Scam Responses* in Selected AP Markets

Area	Topic	Australia	Hong Kong	India	Indonesia	Japan	New Zealand	Singapore	Taiwan
Authentication	Secure out-of-band authentication	✓	✓	✓			✓	✓	
	Multi-factor authentication	✓	✓	✓	✓		✓	✓	✓
	Secure communication	✓		✓		✓	✓	✓	✓
	FI-telco collaboration	✓	✓					✓	
	Digital identity	✓	✓	✓			✓	✓	
	Tokenisation	✓	✓	✓	✓		✓	✓	
Intelligence	Anti-scam centres	✓	✓		✓		✓	✓	✓
	Data exchanges	✓	✓				✓ Pilot	✓	✓
	Industry forums	✓	✓	✓	✓	✓	✓	✓	✓
Consumer Awareness	Payment controls	✓	✓	✓	✓		✓	✓	✓
	Public scam search engines		✓						✓ Pilot
	Public campaigns	✓	✓	✓	✓	✓	✓	✓	✓
Regulatory Frameworks	Liability / Accountability	✓					✓	✓	✓

** This is a non-exhaustive list of anti-scam responses implemented in selected AP markets, which includes regulatory obligations and / or industry initiatives.*

© 2025 Visa. All rights reserved.

Appendix 3: Singapore Case Study

State of Scams in Singapore

In Singapore, scams have become a significant issue, with victims losing record amounts annually, hitting S$1.1 billion[50] in 2024. The most common scam types include job scams, eCommerce scams, fake friend scams, and phishing scams. The Singapore Police Force (SPF) reports that job scams recorded the highest number of cases in 2023, while eCommerce scams were the most common ruse in 2024. Scammers commonly reach out to victims through messaging platforms, social media, phone calls, and online shopping platforms. These methods constitute the top contact methods used by scammers.

Government and Industry Response

In Singapore, the approach[51] towards tackling scams has been multi-layered and wide-ranging, emphasising the importance of the respective roles of consumers and industry stakeholders. In terms of recent developments, the Singapore Government has been emphasising the importance of a whole-of-ecosystem approach to scams, fostering collaboration across multiple government agencies, as well as private sector entities. Equally crucial is an informed and vigilant public, which serves as a cornerstone in the collective fight against scams. Singapore adopts a three-pronged strategy to fight scams, including upstream and downstream measures, as well as public education.

Figure 1: Singapore's Broad Strategy to Combat Scams (source: Monetary Authority of Singapore)

Singapore's Broad Strategy to Combat Scams

Upstream Measures

ScamShield mobile app to filter and block scam messages and calls, and the SMS Sender ID Registry regime to label non-registered senders with the "Likely-SCAM" label.

Downtown Measures

Bank measures implemented to strengthen anti-malware controls, fraud surveillance, and detection capabilities.

Public Education

Public education, through public advisories and sharing best practices to fight scams.

Upstream measures include initiatives like the ScamShield mobile app and the SRF, while downstream measures involve bank safeguards and fraud detection capabilities. Public education efforts focus on community empowerment and scam resilience training for consumers. This multi-pronged approach aims to disrupt scam operations, protect consumers, and create a more scam-resilient Singapore.

International Collaboration

The SPF works closely with foreign counterparts and partners such as the Royal Malaysia Police and INTERPOL to exchange information and conduct joint investigations and operations against transnational scams. For instance, in 2024, the Anti-Scam Centre (ASC) of SPF, in collaboration with Timor-Leste authorities and INTERPOL, made the largest recovery of over US$40 million (approximately S$53 million) in a case of Business Email Compromise Scam.

[50] Singapore Police Force. (2024). Annual scams and cybercrime brief. ScamShield.
[51] Monetary Authority of Singapore. (n.d.). Combatting scams. https://www.mas.gov.sg/regulation/combatting-scams

© 2025 Visa. All rights reserved.

Appendix 4: Australia Case Study

State of Scams in Australia

Scams are a major issue in Australia. While card-not-present (CNP) fraud, which accounts for around 90% of all card fraud in Australia[52], saw strong growth between 2021 and 2023, it is still four times lesser compared to scams[53]. Fraudsters are gravitating towards authorised fraud (scams), as the payoffs can be higher by exploiting human trust. According to data from the Australian Financial Crimes Exchange (AFCX) from the end of the 2022-23 financial year[54], nearly half of all scam losses were processed through cryptocurrency exchanges. Scammers use a range of channels to contact victims, including social media, text, calls, email and mobile applications. According to the latest Targeting Scams report[55] on scams activity in 2024, while social media is the most common reported contact method (overall losses of A$69.5 million), it is phone calls which result in the highest number of actual losses to scammers (A$107.2 million).

Government and Industry Response

Australia's Government and industry are responding to the rise in scams through a multi-faceted approach. Agencies such as the Australian Competition and Consumer Commission (ACCC), through its Scamwatch platform, actively educate the public and provide mechanisms for reporting scams. The ACCC also established the National Anti-Scam Centre (NASC) in July 2023. The Australian Securities and Investments Commission (ASIC) focuses on regulating financial markets and offers consumer education to prevent fraud. Meanwhile, the Australian Cyber Security Centre (ACSC) enhances national cybersecurity, supports individuals and businesses, and facilitates reporting of cyber incidents. Together, these agencies collaborate through task forces and working groups, and policies to stay ahead of scammers.

In parallel, industry efforts play a crucial role in the anti-scam landscape. FIs deploy advanced fraud detection systems and run educational campaigns to inform customers about scam prevention. Telco providers use technology to block scam calls and messages and work collaboratively with government agencies. Retail and eCommerce sectors implement secure payment systems and enhanced customer verification processes. Industry associations create best practice guidelines and facilitate information sharing, while the Australian Banking Association (ABA) Scams Accord exemplifies public-private partnerships and cross-industry collaboration to further strengthen the country's defenses against scams.

International Collaboration

The NASC has placed a secondee at the Joint Policing Cybercrime Coordination Centre and engages internationally in law enforcement, including participating in the Global Fraud Summit in London in March 2024. In December 2024, the Australian Communications and Media Authority (ACMA) and the Office of Communications (Ofcom) announced a new Framework for Practical Cooperation to facilitate mutual assistance and information-sharing to achieve consumer outcomes. This has enabled Australia and the UK to join forces to combat phone scams, spam and unsolicited calls under a new agreement signed by the two markets' communications regulators. Furthermore, AusPayNet, a self-regulatory body for Australia's payments industry, has joined GASA as a Supporting Member[56], with the goal of strengthening its international collaboration and network to combat scams and fraud.

[52] Australian Payments Network. (2023). Fraud statistics for the 2023 calendar year.
[53] National Anti-Scam Centre. (2023). Targeting scams report 2023.
[54] Financial Year in Australia is from 1 July – 30 June
[55] Australian Competition and Consumer Commission. (2024). Targeting scams report 2024.
[56] Global Anti-Scam Alliance. (2023). Australian Payments Network (AusPayNet) joins GASA as a supporting member.

© 2025 Visa. All rights reserved.

How can Visa help?

For more information, please visit our website or contact the Asia Pacific Risk Team: Wanjing Ji (wji@visa.com) or Jie Ying Tan (jietan@visa.com).

© 2025 Visa. All rights reserved.