pwc sumsub SFA SINGAPORE FINTECH ASSOCIATION

Building resilience against scams

Prevention, detection, and awareness



Table of contents

Executive summary

Chapter 1: Scams landscape in Singapore and ASEAN

1.1 Setting the scene: Understanding scams and fraud

1.2 Historical context and evolution of the scam landscape

1.3 Current scam patterns and fraud trends in Singapore and ASEAN

Chapter 2: Regulatory and responsibility landscape

2.1 From consumer vigilance to shared accountability

2.2 Singapore's anti-scam regulatory framework

2.3 Regulatory responses across ASEAN-6 markets

Chapter 3: The rise of AI-enabled fraud

3.1 Rise of synthetic identities and deepfake spoofing

3.2 The obsolescence of legacy and low-effort forgeries

3.3 High-volume persistence—automated retry loops

Chapter 4: Challenges in tackling scams

4.1 Ecosystem coordination challenges

4.2 Human behaviour and victim vulnerabilities

4.3 Crypto as part of the evolving scam ecosystem

Chapter 5: Prevention, response and assurance considerations

5.1 An effective fraud prevention strategy

5.2 Education and awareness

5.3 Assurance and compliance review

Conclusion

Acknowledgements

This report is jointly published by PwC, Sumsub, and the Singapore FinTech Association (SFA), blending regulatory risk expertise, cutting-edge verification tech, and industry advocacy under a shared commitment to strengthen trust. By combining these complementary strengths, we deliver actionable insights to help the digital finance community withstand evolving scams and build long-term resilience.

We would also like to thank the Tech For Good Institute (TFGI) for its perspectives in this report on the evolving conversation on scams, fraud prevention, and digital trust, achieved through its commitment in advancing technology for social good.

Through its commitment to advancing technology for social good, TFGI has helped bring important perspectives to the evolving conversation on scams, fraud prevention, and digital trust.

We are grateful for TFGI's continued support and contribution to this collaborative effort, which has helped strengthen the depth and relevance of the insights presented in this report.



Executive Summary

Scams in Singapore and ASEAN: trends, insights, and strategic remediation



A rising ecosystem risk

Scams have emerged as one of the most significant risks facing consumers, businesses and financial institutions (FIs) across Singapore and ASEAN. Driven by increasing digitalisation, evolving social engineering techniques, and the growing use of emerging technologies, scams have become more sophisticated, scalable, and difficult to detect. What was once largely an issue of consumer awareness has evolved into a broader ecosystem challenge requiring coordinated action from financial institutions, payment service providers, telecommunications operators, digital platforms, regulators, and law enforcement agencies.



Impact across the ecosystem

The impact of scams extends beyond direct financial losses. Consumers face increasingly convincing and technologically advanced fraud attempts, while financial institutions and payment service providers are expected to strengthen anti-scam controls without creating excessive friction for customers. Telecommunications operators and online platforms are also coming under greater scrutiny for their role in detecting, disrupting, and preventing malicious activity. Across ASEAN, the cross-border nature of scam operations continues to present significant challenges for prevention, investigation, and enforcement efforts.



The regulatory response

In response, regulators and industry participants have introduced a range of measures designed to strengthen anti-scam resilience. In Singapore, initiatives such as the Shared Responsibility Framework, the Protection from Scams Act, and anti-scam measures applicable to FIs and Major Payment Institutions (MPIs) seek to improve accountability, strengthen consumer protection, and encourage more effective scam prevention and detection capabilities. Across the region, governments and industry stakeholders are similarly exploring enhanced collaboration, information sharing, and coordinated responses to address increasingly sophisticated scam threats.



About this report

Against this backdrop, this report examines the evolving scam landscape in Singapore and ASEAN, highlighting key scam trends, emerging risks, regulatory developments, and implementation challenges. It also explores the role of technology in both enabling and combating scams, and discusses practical measures that consumers, financial institutions, payment service providers, industry stakeholders, and other ecosystem participants can adopt to strengthen their resilience against fraud and scam-related threats.

1

Scams landscape in Singapore and ASEAN

1.1 Setting the scene: Understanding scams and fraud

1.2 Historical context and evolution of the scam landscape

1.3 Current scam patterns and fraud trends in Singapore and ASEAN

1.1 Setting the scene: understanding scams and fraud



“Scams” and “fraud” are terms that are often used interchangeably, but by definition, are distinct concepts.

Fraud

In literature, fraud is a broad legal category encompassing any act of intentional deception for unlawful gain or to cause harm[1], typically where the victim remains unaware of the deception until the harm has occurred. For example, a company may falsify its financial statements to mislead investors or regulators.

Scams

On the other hand, scams are a specific type of fraud that rely on direct psychological manipulation.[2] Scammers use tactics such as fear, urgency, or emotional appeal to persuade individuals to willingly provide sensitive information, transfer funds, or carry out actions against their own interest. For example, a scammer may impersonate a bank representative and request a transfer of funds.

Both scams and fraud are rooted in deception and cause significant financial and emotional harm. While fraud typically involves manipulation of systems, scams target the individual, exploiting trust and behavioural triggers to achieve their aims.

However, in Southeast Asia, the local terminologies and treatment of scams and fraud often overlap. In fact, there is no standalone legal definition of ‘scams’ that is recognised regionally, and scams are typically prosecuted as a subset of cheating or fraudulent activities. For example, Indonesia broadly uses the word penipuan, which in Bahasa Indonesia refers to both ‘fraud’ and ‘scam’ without distinguishing between specific technical methods. In Singapore, scams and fraud are prosecuted as ‘cheating’ under the Penal Code 1871.[3] The newly enacted Protection Against Scams Law, passed in 2024, reinforces this framework by placing scams under the same cheating provisions set out in the Penal Code.[4] In the Philippines, there is also no legal definition of a scam. Instead, scamming is prosecuted under the offence of Estafa (swindling), as provided for in Articles 315 to 318 of the Revised Penal Code.[5] These same provisions are also applied in cases of fraud, reflecting the overlap in how the two terms are addressed in law.[6]

A compilation of the legal definitions of scams and fraud across Southeast Asia can be found in **Table 1** of Chapter 1.2 in the Tech for Good Institute report, **Building Resilience Against Digitally-enabled Scams and Fraud in Southeast Asia: A Whole-of-Society Approach**.

[1] Fraud and scams: How To Spot The Difference, HSBC UK.
[2] Fraud vs Scams, Explained, Paypal, 13 October 2023.
[3] Penal Code [Penal Code 1871 ss. 415–420A], Singapore Statutes Online, 2020.
[4] Protection from Scams Bill 43 of 2024,Parliament of Singapore, 2024.
[5] Penalties under RPC Articles 315 and 318 for Estafa, Respicio and Co. Law Firm, 17 March 2025.
[6] Legal Advice and Overview on Fraud in the Philippines, Respicio and Co. Law Firm, 14 October 2024.

1.2 Historical context and evolution of the scam landscape

Scams in Singapore and across ASEAN have evolved significantly over the past decade. Historically, scams were often localised and relied on direct forms of deception such as phone calls, impersonation, and fraudulent prize notifications. As internet access, smartphones, digital banking, e-commerce and messaging platforms became more widespread, scammers gained the ability to reach larger victim populations across multiple channels and jurisdictions.

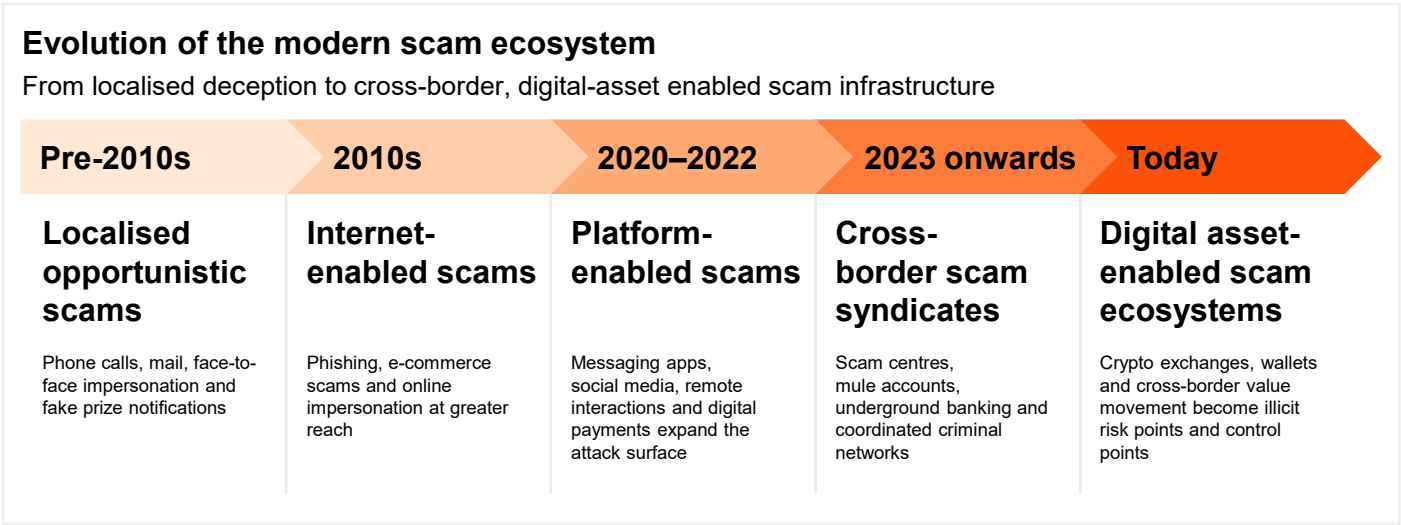


Figure 1: Evolution of the scam landscape in Singapore and ASEAN

Source: PwC analysis based on Singapore Police Force, Annual Scam and Cybercrime Brief 2025; UNODC, Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia (2025);

The evolution of scams broadly mirrors the digitalisation of society. As individuals and businesses increasingly adopt digital services, scam activity evolves from localised deception to platform-based and cross-border fraud conducted through websites, social media platforms, messaging applications, and digital payment channels. More recently, scam activity has become increasingly organised and transnational in nature. According to the United Nations Office on Drugs and Crime (UNODC), scam operations across Southeast Asia have evolved beyond isolated criminal activities into sophisticated ecosystems involving scam centres, underground banking networks, illicit online marketplaces, and other service providers that facilitate the movement of illicit funds across multiple jurisdictions.[7]

This is consistent with PwC's Annual Threat Dynamics 2026, which observed that financial crime, insider risk and socially engineered fraud have increasingly merged into a single threat ecosystem, as threat actors exploit identities, trust relationships and digital platforms to scale attacks across multiple channels and jurisdictions.[8]

The digital asset dimension. A growing feature of these evolving scam ecosystems has been the use of digital assets. Beyond investment scams, organised criminal networks increasingly utilise a combination of traditional financial channels, mule account networks and digital assets to move illicit proceeds across jurisdictions, further complicating detection, intervention and recovery efforts.

[7] Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia, United Nations Office on Drugs and Crime, 2025.
[8] Annual Threat Dynamics 2026, PwC, 2026.

1.2 Historical context and evolution of the scam landscape

Recent scam trends in Singapore

In Singapore, scam-related harm remains significant despite recent improvements in reported scam trends. According to the Singapore Police Force, while scam and cybercrime cases reached 55,810 in 2024,[9] scam cases fell by 27.6% to 37,308 cases in 2025.[10] Scam losses decreased by 17.9% from approximately S$1,112 million in 2024 to approximately S$913.1 million in 2025. Cryptocurrency-related losses accounted for approximately S$182.2 million, representing around 20.0% of total scam losses reported in 2025.

28% YoY decrease in scam cases (2025)

18% YoY decrease in scam losses (2025)

20% of total scam losses were crypto-related (2025)

Impact lens

Losses Exposure Disputes

The numbers are selected to show scale, complexity and institutional pressure, not to reproduce every statistic.

Scale	Complexity	Pressure
S$913.1m reported scam losses	**S$182.2m** crypto-related losses	**1,285** fraud/scam dispute claims
Losses remained substantial in 2025 despite declining from the 2024 record level.	About 20.0% of total scam losses involved cryptocurrencies, adding tracing and recovery complexity.	Fraud and scam related claims handled by FIDReC rose 55% and accounted for nearly half of claims handled.

Figure 2: Scam-related harm and financial sector impact in Singapore (2025)

Source: Singapore Police Force, Annual Scam and Cybercrime Brief 2025; Financial Industry Disputes Resolution Centre Ltd, FY2024/2025 Claims Statistics.

Beyond consumer losses, scams increasingly present operational, regulatory, and trust-related challenges for FIs and payment service providers. The Financial Industry Disputes Resolution Centre Ltd (FIDReC), Singapore's independent dispute resolution institution for consumers and FIs, reported that it received 4,355 claims in FY2024/2025, with 2,646 claims accepted for handling. Fraud and scam-related disputes rose to 1,285 claims, representing a 55% increase and accounting for nearly half of all claims handled by FIDReC.[11] These developments highlight the growing pressure on FIs to strengthen controls, manage scam-related disputes, and demonstrate effective customer protection measures. While Singapore has recorded reductions in reported scam cases and losses, the persistence of significant financial losses and rising scam-related disputes demonstrates that scams remain an ongoing challenge for the financial sector.

[9] Annual Scams and Cybercrime Brief 2024, Singapore Police Force, 25 February 2025.
[10] Annual Scams and Cybercrime Brief 2025, Singapore Police Force, 25 February 2026.
[11] FY2024/2025 Claims Statistics, Financial Industry Disputes Resolution Centre Ltd., 26 November 2025.

1.3 Current scam patterns and fraud trends in Singapore and ASEAN

Fraud trends across selected ASEAN jurisdictions

As scams and fraud continue to evolve across the region, understanding broader regional fraud trends provides important context for the scam typologies affecting consumers, Fis, and other ecosystem participants today. Table 1 presents selected ASEAN jurisdictions, allowing for a comparison of fraud exposure and readiness across key markets in the region. To contextualise the regional fraud landscape, the analysis draws on the Global Fraud Index 2025 by Sumsub, a global verification and anti-fraud platform. The Index assesses 112 countries across four key pillars, namely fraud activity, resource accessibility, government intervention, and economic health, to evaluate both fraud risk and a country's readiness to access KYC and AML services.[12] Consistent with the distinction outlined in Section 1.1, the Global Fraud Index captures a broader range of fraud-related risks and indicators beyond scam incidents alone, providing additional context on the fraud landscape across the selected jurisdictions.

Country	Fraud Index	Fraud Activity	Resource Accessibility	Government Intervention	Economic Health
Singapore	1.36 ▲	0.89 ▲	0.33 ▲	0.08 ▼	0.31
Malaysia	3.47 ▲	2.07 ▲	1.3 ▲	0.47 ▲	0.46 ▲
Thailand	2.03 ▼	0.5 ▼	1.46 ▲	0.57	0.39 ▲
Indonesia	6.53 ▲	4.93 ▲	1.73 ▲	0.57 ▲	0.46 ▲
Philippines	3.38	1.58	1.69	0.68	0.43
Cambodia	3.43 ▼	0.9 ▼	1.81 ▼	1.07 ▲	0.4 ▲
Vietnam	4.15	2.39	1.55	0.66	0.44
Global Average	**2.79**	**2.07**	**1.38**	**0.65**	**0.46**

▲ Increased from 2024 ▼ Decreased from 2024

Table 1: Sumsub Global Fraud Index across selected ASEAN jurisdictions (2025)

Source: Sumsub Global Fraud Index, 2025.

Analysis of the 2024 and 2025 Global Fraud Index data indicates an overall reduction in fraud index scores across the selected ASEAN jurisdictions presented in Table 1. At the same time, fraud activity increased in most jurisdictions included in the analysis, with Thailand being a notable exception. According to Sumsub, this trend suggests that while anti-fraud awareness and resilience may be improving in some areas, fraud remains a persistent and evolving threat.

[12] Global Fraud Index 2025, Sumsub.

1.3 Current scam patterns and fraud trends in Singapore and ASEAN

Common scam types across the region

Several scam types continue to be commonly observed across Singapore and Southeast Asia. While the methods employed by fraudsters vary, many scams rely on a combination of social engineering, impersonation, deception, and technology to manipulate victims and facilitate the movement of illicit funds. The six scam types most commonly observed in the region are phishing, impersonation of authority, romance, fake friend, employment, and deepfake scams. Table 2 provides an overview of each scam type and its key characteristics.

Type of scam	Description
Phishing scam	Phishing scams represent fraudulent attempts to obtain sensitive information (such as login credentials, banking details, or Transaction Authorisation Codes) by masquerading as trustworthy entities. These schemes typically appear through email, text messages, or instant messaging platforms such as WhatsApp, exploiting the ubiquity of digital communication.
Impersonation of authority scam	Impersonation scams involve fraudsters posing as trusted authority figures, such as government officials, police officers, or corporate representatives, to manipulate victims into complying with fraudulent requests. These schemes exploit fundamental human psychology, particularly our ingrained respect for authority and tendency to comply with official directives. Perpetrators typically construct elaborate scenarios designed to invoke fear, urgency, or concern about legal consequences. Common narratives include claims of unpaid fines, involvement in criminal investigations, or urgent administrative issues requiring immediate attention.
Romance scam	Romance scams target individuals seeking emotional or romantic connections, exploiting the vulnerability inherent in the human desire for companionship and affection. These schemes often begin on online platforms, including dating applications and social media networks, where scammers can easily create elaborate false identities. They typically pose as attractive, successful professionals such as doctors, engineers, or military personnel, using these fabricated identities to gain trust and admiration while offering plausible reasons for limited communication or an inability to meet in person.

Table 2: Six common threats across the regional scam and fraud landscape

Source: Compiled by Tech For Good Institute, 2025 [13]

[13] Building Resilience Against Digitally-enabled Scams and Fraud in Southeast Asia: A Whole-of-Society Approach, Tech For Good Institute, September 2025.

1.3 Current scam patterns and fraud trends in Singapore and ASEAN

Table 2: Six common threats across the regional scam and fraud landscape (continued)

Type of scam	Description
Fake friend scam	Fake friend scams exploit the trust built into personal relationships by utilising compromised or fabricated social media accounts that mimic those of victims' friends, family members, or acquaintances. Because the messages appear to come from known contacts, they allay the victims' natural scepticism and increase the likelihood of compliance.
Employment scam	Employment scams target vulnerable individuals with false promises of lucrative employment opportunities, often requiring upfront payments for processing fees, training costs, or travel documentation. These schemes frequently serve as fronts for human trafficking networks, exploiting desperation for better economic opportunities.
Deepfake scam	Deepfake scams represent one of the most technologically advanced forms of fraud, utilising Artificial Intelligence (AI) to create highly realistic yet entirely fabricated audio or video content. These schemes typically involve impersonating public figures or trusted individuals to promote fraudulent investment opportunities, products, or services.

[16] Fake Friend Scam, CelcomDigi, 5 August 2024.
[17] Jobs and employment scams, ScamWatch.
[18] Major Regulatory Alerts About AI and Deepfake Fraud Signal Significant Challenge to 2025 Digital Account Growth, Feedzai, 16 December 2024.

1.3 Current scam patterns and fraud trends in Singapore and ASEAN

Scam exposure and victimisation in Singapore

A survey was conducted in September 2024 by TFGI in collaboration with Bamboo Builders, to understand exposure to and behaviour regarding scams and fraud. The study had a sample of 1,000 respondents representing the general population in Singapore, including citizens and permanent residents, from 10 to 74 years old. Interviews were done via online surveys for 800 respondents aged 18 to 74 years old, and via face-to-face street intercepts for 200 respondents aged 10 to 17 years old. Further quotas were set for the latter group: 75 for those aged 10 to 12, and 125 for those aged 13 to 17.



have fallen victim to an online scam in Singapore

General population

97% **are concerned about scam prevalence**

49% **of the 18–34 working age group were scammed**

64% **of the 18–34 working age group know a victim**

The survey found that in Singapore, 1 in 3 respondents have fallen victim to an online scam, and 97% profess concerns about the prevalence of scams in the country. The working-age group (18–34 years old) is the most vulnerable, with 49% being scammed themselves, and 64% knowing someone who has been scammed.[14]

The prevalence of these scam types highlights the diverse methods employed by fraudsters to target individuals across the region. While scam techniques continue to evolve alongside technological and behavioural changes, many remain rooted in social engineering, deception, and the exploitation of trust. Understanding these prevailing scam patterns provides important context for the broader challenges associated with preventing, detecting, and responding to scams across Southeast Asia.

[14] Strengthening Scam Readiness in Singapore, Bamboo Builders, 2025.

2

Regulatory and responsibility landscape

2.1 From consumer vigilance to shared accountability

2.2 Singapore's anti-scam regulatory framework

2.3 Regulatory responses across ASEAN-6 markets

2.1 From consumer vigilance to shared accountability



The regulatory shift

As scam typologies evolve in scale, speed, and sophistication, regulatory responses are increasingly moving beyond consumer education alone towards clearer allocation of responsibilities across the wider digital and financial ecosystem. This shift reflects a growing recognition that scams often involve multiple actors, channels, and systems, including FIs, payment service providers, telecommunications providers, digital platforms, regulators, and law enforcement agencies. This chapter examines how regulatory and policy responses in Singapore and ASEAN are evolving, and what these developments mean for FIs and major payment institutions in strengthening scam prevention, intervention, and recovery capabilities.

Historically, scam prevention efforts were often framed around consumer awareness and individual vigilance. Consumers were encouraged to recognise suspicious links, verify unusual requests, avoid sharing credentials, and report suspected scams promptly. While consumer awareness remains important, modern scams increasingly involve multiple actors, channels, and systems, making it difficult for any single party to see the process of a scam from end to end or to disrupt it.

A scam may begin through a phishing link, impersonation call, social media advertisement, or messaging platform, before moving into bank transfers, e-wallet payments, mule accounts, cryptocurrency channels, or cross-border fund flows. This has led regulators to place greater emphasis on shared responsibility, where consumers, FIs, payment service providers, telecommunications providers, digital platforms, and enforcement agencies each play a role in prevention, detection, intervention, and recovery. Singapore's move towards shared accountability reflects a broader global shift towards more coordinated approaches to risk management. PwC's 2026 Global Digital Trust Insights similarly highlights how growing ecosystem complexity and dependencies across interconnected stakeholders are creating new risk management challenges for organisations, reinforcing the need for coordinated approaches to prevention and response.[15]

This shift towards shared accountability is particularly relevant for FIs and major payment institutions, as scam-related risk can arise across multiple points of the customer and transaction lifecycle. Anti-scam risk management is therefore no longer only a fraud operations issue. It is increasingly becoming a governance, compliance, customer protection, and operational resilience priority.

Against this backdrop, FIs, payment service providers, telecommunications operators, digital platforms, regulators, and law enforcement agencies are increasingly expected to collaborate and coordinate their efforts. The following sections examine how these stakeholders are evolving their roles and responsibilities to strengthen scam prevention, detection and response capabilities.

[15] Global Digital Trust Insights 2026, PwC, 2026.

2.2 Singapore's anti-scam regulatory framework

In Singapore, the shift towards ecosystem accountability is reflected in five key anti-scam measures and regulatory frameworks, each addressing a different part of the scam response chain. The Monetary Authority of Singapore (MAS) Circular on Anti-scam Measures by Major Payment Institutions Providing Personal Payment Accounts that Contain E-money (MPI Anti-Scam Circular) focuses on preventive safeguards within e-wallet and payment account ecosystems. The MAS Shared Responsibility Framework clarifies roles and responsibility allocation for in-scope scam losses. Finally, the Protection from Scams Act 2025 (PSA) provides a legislative mechanism for earlier intervention in ongoing scam situations. These measures are complemented by the MAS E-Payments User Protection Guidelines, which set out expectations for protections against unauthorised transactions, as well as broader AML/CFT requirements that support the detection, prevention, and reporting of suspicious activities associated with scams.

Measure	Applicability	Key features	Relevance to FIs/MPIs
MPI Anti-Scam Circular MAS Circular on Anti-scam Measures by Major Payment Institutions Providing Personal Payment Accounts that Contain E-money	MPIs providing personal payment accounts containing e-money and their customers[16]	Wallet and transaction thresholds, customer notifications, cooldown periods, and additional verification or friction at high-risk events	Raises expectations for MPIs to embed scam safeguards into product design, transaction controls, customer alerts, and incident response processes
MAS Shared Responsibility Framework	Account users, Responsible FIs (banks and relevant PSPs) and responsible telecommunications companies[17]	Clarifies the roles and accountabilities of account users, responsible FIs and responsible telecommunications companies in relation to specified phishing scam losses and seemingly authorised transactions	Reinforces that scam prevention is not solely a consumer obligation. FIs and payment service providers are expected to maintain effective controls, detection, notification and escalation mechanisms
Protection from Scams Act 2025	Individuals at risk of scam-related fund transfers and banks required to implement restriction orders[18]	Empowers specified officers to issue restriction orders to banks, temporarily restricting certain transfers, withdrawals, and credit facility use where relevant conditions are met	Supports intervention before losses escalate, particularly where there is reasonable belief that an individual may transfer money to scammers or draw down credit facilities for the benefit of scammers

Table 3: Key Singapore anti-scam measures

[16] Circular on Anti-scam measures by Major Payment Institutions Providing Personal Payment Accounts that contain E-money, Monetary Authority of Singapore, 25 October 2024.
[17] Guidelines on Shared Responsibility Framework, Monetary Authority of Singapore, 24 October 2024.
[18] Protection from Scams Act 2025, Singapore Statues Online, 21 February 2025.

2.2 Singapore's anti-scam regulatory framework

Table 3: Key Singapore anti-scam measures (continued)

Measure	Applicability	Key features	Relevance to FIs/MPIs
E-Payments User Protection Guidelines	Responsible FIs, including banks and relevant payment service providers offering protected accounts to individuals and sole proprietors[19]	Establishes responsibilities of account holders and FIs, sets expectations for transaction alerts, cooling-off periods, kill switches, unauthorised transaction investigations, liability allocation, and dispute resolution processes	Strengthens customer protection and unauthorised transaction management by requiring safeguards, investigation procedures, and clear accountability frameworks for handling disputed transactions
MAS anti-money laundering (AML)/ countering the financing of terrorism (CFT) regime	MAS-regulated FIs, including banks, payment service providers, capital markets intermediaries, insurers and other regulated FIs[20]	Requires risk-based AML/CFT controls, customer due diligence (including identification of beneficial owners), ongoing monitoring, regular account reviews, suspicious transaction reporting, targeted financial sanctions screening and compliance with MAS AML/CFT notices and guidelines	Strengthens FIs' ability to detect, deter, and report illicit fund flows associated with scams, money laundering, and other financial crimes, while supporting a coordinated industry-wide approach to financial crime risk management



Is your organisation ready?

- Who owns scam risk across your organisation, and is that accountability clearly defined?
- Are your controls keeping pace with evolving regulatory expectations and scam types?
- Could your organisation intervene early enough to prevent a scam loss before it occurs?

[19] MAS E-Payments User Protection Guidelines, Monetary Authority of Singapore, 28 September 2018.
[20] Anti-Money Laundering, Monetary Authority of Singapore.

2.3 Regulatory responses across ASEAN-6 markets

Why the regional view matters

01	**Prevention**
02	**Responsibility allocation**
03	**Intervention**

Singapore's anti-scam measures reflect a progressively more structured regulatory approach, where scam risk is addressed across prevention, responsibility allocation, and intervention. Rather than treating scams solely as isolated fraud incidents or matters of consumer vigilance, the framework places greater emphasis on the role of ecosystem participants in reducing scam exposure, responding to suspicious activity and supporting earlier intervention where customers remain at risk.

This approach is particularly relevant given the cross-border nature of modern scam activity. As discussed in the first chapter, scams affecting consumers in one jurisdiction may involve scam syndicates, digital platforms, payment channels, mule accounts, or fund flows located elsewhere. Accordingly, while Singapore provides a useful example of a more developed domestic anti-scam framework, the broader regulatory landscape also needs to be considered at the ASEAN level, where policy coordination and regional anti-scam guidance continue to develop.

While this report examines scam trends and prevention measures across Singapore and the broader ASEAN region, the regulatory analysis in this chapter focuses specifically on the six largest ASEAN economies (ASEAN-6): Indonesia, Malaysia, the Philippines, Singapore, Thailand and Vietnam. This narrower scope reflects the relative maturity and availability of regulatory frameworks within these jurisdictions and is intended solely for the purposes of this regulatory review.

Across ASEAN, jurisdictions are adopting different regulatory approaches to address scam and fraud risks, reflecting variations in domestic legal frameworks, enforcement arrangements, financial sector structures, and scam risk profiles. These frameworks differ in scope and design, but they address comparable areas of concern, including scam reporting, fund tracing, mule account management, cybercrime enforcement, financial account protection, anti-fraud governance, and digital banking security.

2.3 Regulatory responses across ASEAN-6 markets

With Singapore's anti-scam framework addressed in the previous section, Table 4 focuses on selected anti-scam and anti-fraud frameworks adopted across the remaining ASEAN-6 jurisdictions.

Jurisdiction	Selected framework/ measure	Key focus	Regulatory/responsibility emphasis
Malaysia	**Policy Document on Ensuring Fair Treatment for Victims of Unauthorised e-Banking Transactions (SEFT)**	Introduced by Bank Negara Malaysia (BNM) to ensure fair treatment of victims of unauthorised e-banking transactions through a structured framework for investigation, dispute resolution, and compensation assessment[21]	Shared accountability between banks and customers based on their respective obligations and conduct
Thailand	**Royal Decree on Measures for the Prevention and Suppression of Technology Crimes (No. 2) B.E. 2568 (2025)**	Introduced by the Thai Government with support from the Bank of Thailand (BOT) to strengthen protection against technology-enabled scams. Requires FIs, payment service providers, and other relevant service providers to implement enhanced fraud controls, including measures relating to impersonation risks, mule accounts, and scam detection[22]	Shared responsibility and greater accountability for regulated service providers that fail to meet prescribed anti-scam obligations
Philippines	**Anti-Financial Account Scamming Act (AFASA) and Bangko Sentral ng Pilipinas (BSP) implementing rules**	The BSP describes AFASA and its implementing regulations as a framework to prevent, detect, and delay fraudulent transactions, trace, hold, verify and recover disputed funds, and support access to financial account information for law enforcement purposes[23]	Financial account protection, fund holding/recovery, information sharing and fraud response involving BSP-supervised institutions.

Table 4: Regulatory frameworks across ASEAN-6 markets

[21] Fraud Resolution: Building Trust through Shared Accountability, Bank Negara Malaysia.
[22] BOT to hold financial institutions liable for call centre scam losses, The Nation Thailand, 14 April 2025.
[23] Anti-Financial Account Scamming Act (AFASA) and Implementing Rules and Regulations (IRR), BSP, 2025.

2.3 Regulatory responses across ASEAN-6 markets

Table 4: Regulatory framework across ASEAN-6 markets (continued)

Jurisdiction	Selected framework/ measure	Key focus	Regulatory/ responsibility emphasis
Indonesia	**Otoritas Jasa Keuangan (OJK) Regulation No. 12 of 2024 on Anti-Fraud Strategy for Financial Services Institutions**	OJK materials state that the regulation requires financial services institutions to strengthen internal controls and apply anti-fraud strategies based on four pillars: 1. Prevention 2. Detection 3. Investigation, reporting, and sanctions 4. Monitoring, evaluation, and follow-up[24]	Internal anti-fraud governance, control effectiveness, investigation, reporting, and monitoring obligations across financial services institutions
Vietnam	**Circular 77/2025/TT-NHNN (amending Circular 50/2024/TT-NHNN on security and safety requirements for online services in the banking sector)**	Introduced by the State Bank of Vietnam (SBV) to strengthen the security and safety of online banking services in response to emerging cyber-enabled fraud risks, including deepfakes, malware, and fraudulent corporate accounts, through enhanced biometric authentication, anti-spoofing controls, and cybersecurity requirements[25]	Preventive digital banking controls, authentication safeguards, and cyber-fraud risk mitigation

[24] Penerapan Strategi Anti Fraud Bagi Lembaga Jasa Keuangan, Otoritas Jasa Keuangan, 2024.
[25] Circular 77/2025/TT-NHNN: Strengthening security requirements for banking services, Dentons LuatViet, 22 April 2026.

2.3 Regulatory responses across ASEAN-6 markets



What the comparison tells us

The selected examples show that ASEAN jurisdictions are strengthening anti-scam and anti-fraud responses, but through different regulatory designs. Some markets place greater emphasis on scam-reporting infrastructure and fund tracing, while others focus on cybercrime enforcement, financial account protection, internal anti-fraud governance, or digital banking security. This reflects the different legal, institutional, and market contexts across the region.

At the same time, the comparison highlights a common implementation challenge—scam activity is increasingly cross-border, while regulatory frameworks remain largely domestic. For FIs and payment service providers operating across ASEAN, this means anti-scam readiness cannot be assessed only by reference to local compliance obligations. Institutions may need to develop internal anti-scam capabilities that are sufficiently consistent across markets, while remaining adaptable to local regulatory requirements. This includes governance, customer onboarding, fraud surveillance, transaction monitoring, mule account detection, customer intervention, dispute handling, and recovery processes.

Capabilities requiring consistency across markets

Governance	**Customer onboarding**	**Fraud surveillance**	**Transaction monitoring**
Mule account detection	**Customer intervention**	**Dispute handling**	**Recovery processes**

Chapter 2 takeaway

Regulatory expectations are moving beyond consumer vigilance alone, towards a more coordinated model of prevention, accountability and intervention across the scam lifecycle.

3

The rise of AI-enabled fraud

3.1 Rise of synthetic identities and deepfake spoofing

3.2 The obsolescence of legacy and low-effort forgeries

3.3 High-volume persistence — automated retry loops

3.1 Rise of synthetic identities and deepfake spoofing

The evolution of fraud in the Asia Pacific region reflects a fundamental paradigm shift—cheap, low-effort tactics are dying out, replaced by sophisticated, AI-driven impersonation and persistent automated attacks. As defence systems evolve, fraudsters are splitting their investments between hyper-realistic synthetic assets and high-volume, automated trial-and-error strategy. Among these emerging threats, the most dramatic shift in Asia Pacific's threat landscape is the proliferation of AI-powered identity manipulation. Deepfake videos and synthetic profiles are rapidly outrunning traditional single-layer verification controls.

AI-powered identity manipulation is rapidly outrunning traditional single-layer verification controls.

35.4%

+73% YoY

Selfie and biometric fraud

Emerging as the single largest threat vector in the region, selfie-related fraud accounted for 35.4% of total fraud cases in 2025—representing a 73% increase compared to 2024 (+6.8 percentage points in overall market share).[26] Fraudsters use real-time deepfake videos and face swaps to mask advanced attacks as routine image mismatches, easily bypassing systems that rely solely on basic image matching or surface-level liveness detection.

+142%

15.7% of fraud

Synthetic personal data

Fabricated identity attacks jumped by 142% compared with 2024, now representing 15.7% of all recorded fraud.[27] Rather than relying entirely on stolen credentials, bad actors blend AI-generated details—such as fake names, addresses, and birth dates—with deepfake media to create completely artificial personas. These synthetic identities are designed to appear internally consistent, easily tricking verification pipelines that lack cross-referencing, network-level analysis, or behavioural biometrics.

Sumsub survey | August 2026

33%	AI-generated documents or profiles
18%	deepfake images, videos, or cloned voices
65%	fraud involving an AI agent

According to a Sumsub survey conducted in August 2026 among business and consumer respondents across Singapore, the Philippines, Indonesia, and Thailand, 33% of businesses experienced confirmed or suspected fraud involving AI-generated documents or profiles, and 18% encountered deepfake images, videos, or cloned voices. Separately, 65% of all surveyed businesses reported confirmed or suspected fraud involving an AI agent.

Looking ahead

54% expect AI-generated identities and documents to be among the fastest-growing fraud threats over the next two years

45% expect deepfake impersonation to grow.

[26] Identity Fraud Report 2025-2026, Sumsub, 25 November 2025.
[27] Ibid.

3.2 The obsolescence of legacy and low-effort forgeries

As AI capabilities become democratised, traditional and manual fraud techniques are collapsing under the weight of modern automated defences.

Dwindling crude tactics[28]

↓ 50%

Blacklist violations plummeted by 50% YoY (a 9.1 pp share drop)

↓ 11%

Basic forged physical IDs dropped 11% YoY (a 4.1 pp share drop)

pp = percentage points



Defensive success vs. threat reallocation

Crude methods like low-resolution scans, simple cut-and-paste document edits, and known bad-actor credentials are no longer effective against modern verification engines.

While this shift significantly reduces operational noise and manual review volume for security teams, it signals a dangerous reality—fraudsters aren't stopping, they are simply reallocating their budgets into advanced generative tools.

[28] Ibid.

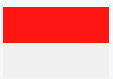
3.2 The obsolescence of legacy and low-effort forgeries

ASEAN snapshot: where fraud is shifting

The increasing sophistication of scams and fraud presents a growing challenge for organisations attempting to prevent, detect and respond to fraudulent activity. According to Sumsub, fraud patterns across APAC have shifted away from traditional techniques towards increasingly sophisticated, AI-enabled methods.

Selfie-related fraud is now the most prevalent fraud type at 35.4% of cases (+73% YoY) and synthetic personal data fraud rose 142% YoY to 15.7% of cases, while blacklist violations (–50%) and forged identity documents (–11%) continue to fall away.

Based on Sumsub's analysis of APAC fraud trends between 2024 and 2025, fraud rates across ASEAN markets showed divergent trajectories, with some jurisdictions experiencing sharp increases while others recorded declines.



Highest fraud rate

Indonesia 5.6% **–7% YoY** ▼

Expansive e-commerce platforms and super-app ecosystems generate ongoing exposure to threats. Notably, deepfakes now represent 5% of all fraud attempts, positioning Indonesia as a primary testing ground for AI-driven onboarding attacks.



Fastest rise

Malaysia 4.0% **+197% YoY** ▲

Cybercriminals exploiting online transactions via money mules, and orchestrating investment scams aimed at expatriates, retirees, and young professionals.



Sharpest fall

Singapore 1.0% **–12% YoY** ▼

Regulatory tightening—such as MAS's enhanced anti-scam and e-payment frameworks—has contributed to these declines. However, a key paradox remains. Despite lower overall fraud volumes, the proportion of deepfake-driven attacks is expanding. In Singapore, deepfake cases surged +158% YoY, primarily propelled by impersonation schemes and fraudulent e-wallet creation. This pattern mirrors a broader trend across developed Asia Pacific economies: declining fraud quantity paired with escalating technical sophistication.



Myanmar 4.8% **+112% YoY** ▲



Laos 2.7% **+74% YoY** ▲

Both emerging markets remain susceptible to fraudulent activity as swift digitalisation exposes systemic vulnerabilities. These nations demonstrate how cybercriminals systematically target and exploit the most vulnerable segments of the Asia Pacific digital landscape.



Philippines 3.1% **+12% YoY** ▲

Fraudulent activity remains high across the region, primarily propelled by vulnerability in remittance platforms, gaming platforms, and social media-integrated onboarding processes—all of which serve as frequent targets for attackers.



Cambodia 2.5% **–5% YoY** ▼

One of the few markets to record a decline, as regulatory tightening across the region begins to take effect.

3.3 High-volume persistence — automated retry loops

Alongside sophisticated media generation, attack patterns reveal a move toward systematic operational volume. Fraudsters are pairing deepfake technology with persistent retry loops for a chance to bypass and leverage system vulnerabilities.



+388%

Year-on-year surge

Persistent resubmissions

Duplicate submissions escalated drastically, quadrupling with a +388% YoY surge, while explicit liveness bypass attempts saw a parallel rise.

Resilience as a weapon

These retry loops demonstrate that bad actors are willing to hammer verification flows continuously. By running high-volume automated loops with slight variations of AI-generated assets, they aim to fatigue risk engines until a single fraudulent attempt slips through.

How automated retry loops work

01 **High-volume automated loops**

02 **Slight variations of AI-generated assets**

03 **Verification flows hammered continuously**

04 **A single fraudulent attempt slips through**

Modern fraud in Asia Pacific is no longer a game of simple deception, but an enterprise-grade threat. Adversaries are pairing hyper-realistic generative assets with relentless brute-force automation, creating a high-volume, high-sophistication challenge that static defences can no longer contain.

4

Challenges in tackling Scams

4.1 Ecosystem coordination challenges

4.2 Human behaviour and victim vulnerabilities

4.3 Crypto as part of the evolving scam ecosystem

4.1 Ecosystem coordination challenges

Challenge 1:

Fragmented stakeholder responsibilities

The diversity in country-specific definitions is symptomatic of fragmented efforts to address scams and fraud. At the national level, multiple agencies and stakeholders operate in parallel. Police forces, telecommunications regulators, FIs, digital platforms, and financial authorities each oversee different aspects of scam response.[29] This frequently results in overlapping mandates, unclear referral processes, and inconsistent support for victims.

Challenge 2:

Cross-border coordination barriers

Outdated legal frameworks and regulatory limitations further hamper cross-border collaboration. Many scams are transnational, involving perpetrators in one country, targeting victims in another, and digital infrastructure hosted elsewhere. Yet national law enforcement agencies often lack the legal authority or operational capacity to act beyond their jurisdictions. Legal inconsistencies, limited diplomatic coordination, and the absence of shared protocols may slow down joint investigations.[30]



Why this matters?

The need for stronger ecosystem coordination is not unique to ASEAN. Globally, scam and fraud threats are becoming increasingly interconnected, often involving multiple actors, channels and jurisdictions. PwC's Annual Threat Dynamics 2026 observed that theft, fraud and insider compromise have increasingly merged into a single convergent threat category, with adversaries combining social engineering, deepfake impersonation, third-party compromise and embedded insider access to target organisations. This highlights the need for greater coordination across stakeholders, particularly where scam activity spans multiple organisations, platforms and jurisdictions.[31]

[29] Building resilience against Scams and Fraud: Spotlight on Malaysia, Tech for Good Institute, 14 April 2025.
[30] From fake jobs to crypto fraud: Why scam gangs in Southeast Asia are a growing global threat, Griffith University, 19 May 2025.
[31] Annual Threat Dynamics 2026, PwC, 2026.

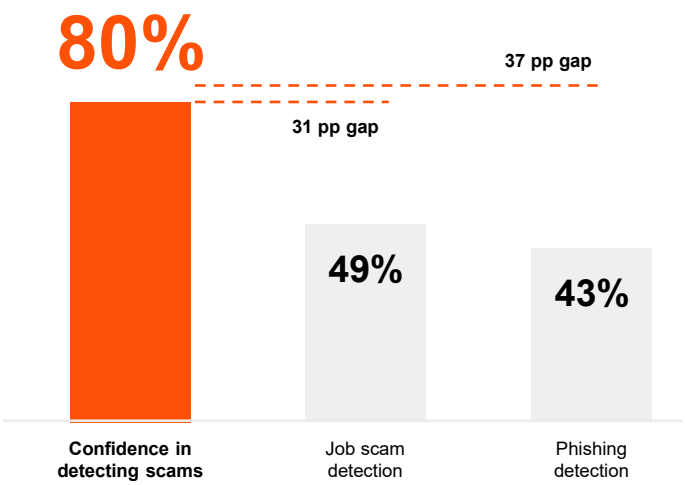
4.2 Human behaviour and victim vulnerabilities

Key insight

More than 80% of Singapore respondents are confident in detecting scams, yet fewer than half correctly identify job scams **(49%)** and phishing emails **(43%)** when tested.

The confidence gap

Confidence does not always translate into actual ability.



pp = percentage points

Recovery preparedness



Singaporeans have a plan in place to recover assets in the event of a scam.

Most rely on financial institutions and the police in their response plan.

Despite growing public awareness of scams, victimisation remains prevalent. Scam tactics frequently exploit human psychology, including trust, fear, urgency, emotional attachment, and the perception of financial gain. As a result, raising awareness alone may not always translate into safer behaviours or better scam detection outcomes.

According to Bamboo Builders and TFGI's September 2024 survey, there is a gap between confidence and actual ability in detecting scams. While over 80% of surveyed respondents express confidence when tested, less than half are able to successfully detect job scams (49%) and phishing emails (43%).[32]

Personal circumstances, such as financial distress or perceived greed, are cited as top reasons for victims falling for phishing, job, e-commerce, and investment scams. Conversely, for fake friend and romance scams, emotional manipulation is recognised as the primary reason why people are victimised. Two in three Singaporeans have a plan in place to recover assets in the event of a scam, with the majority being reliant on FIs and the police in their scam response plan.[33]

Among respondents who indicated they had a recovery plan, the most commonly cited steps included contacting their bank or FI, freezing affected accounts or cards, and filing a police report. These findings suggest that many consumers view FIs and law enforcement as key participants in their response and recovery efforts following a scam incident.

[32] Strengthening Scam Readiness in Singapore, Bamboo Builders, 2025.
[33] Ibid.

4.3 Crypto as part of the evolving scam ecosystem

Crypto has become an increasingly important part of the broader fraud and scam landscape. Its speed, cross-border reach, and digital-native infrastructure can make crypto services attractive targets for fraudsters and useful channels within wider scam operations. The risk is therefore not limited to fraudulent crypto transactions themselves—it can begin with a compromised, stolen, or synthetic identity and continue through account creation, social engineering, mule activity, and the movement of illicit funds, just as observed among fiat transactions within traditional Fis.

Sumsub's State of the Crypto Industry 2026 shows that this threat environment intensified significantly in Asia Pacific in 2025. The fraud rate among crypto businesses in Asia Pacific increased from 2.0% in 2024 to 3.3% in 2025, a 65% year-on-year rise. This occurred while the global crypto fraud rate remained unchanged at 2.2%, making Asia Pacific's increase particularly notable.[34]

The scale of legitimate crypto activity further raises the importance of detecting these patterns without creating unnecessary friction. Sumsub data shows that 94% of legitimate Asia Pacific users successfully completed crypto verification in 2025, up from 93% in 2024, even as regional fraud increased sharply. This demonstrates that stronger fraud controls do not necessarily have to come at the expense of legitimate customer conversion.

The numbers

3.3% — **APAC crypto fraud rate**
Up from 2.0% in 2024 — a 65% rise, while the global rate held flat at 2.2%.

94% — **Verification success**
Legitimate APAC users completing crypto checks in 2025, up from 93%.

44% — **Company share of value**
Up from 4% in 2024; company-to-company activity grew from 1% to 12% of transactions.

The implication for FIs and crypto businesses is that onboarding and transaction monitoring should not operate as separate lines of defence. Identity signals established during verification should be connected with subsequent device, behavioural and transaction activity. Suspicious changes in behaviour, links between apparently unrelated accounts, unusual transaction patterns, and indicators of mule activity can then be assessed as part of the customer's broader risk profile.

This is increasingly important as crypto itself becomes more institutional. Sumsub's 2025 data shows that company-to-company activity grew from **1% to 12%** of transactions, while companies' share of transaction value increased from just **4% in 2024 to 44% in 2025**. As higher-value business flows expand alongside retail activity, effective scam prevention will increasingly depend on connecting identity verification, business verification, behavioural intelligence, and transaction monitoring throughout the customer lifecycle, rather than treating fraud as a problem that can be addressed at a single checkpoint.

[34] State of the Crypto Industry 2026, Sumsub, March 2026.

5

Prevention, response and assurance considerations

5.1 An effective fraud prevention strategy

5.2 Education and awareness

5.3 Assurance and compliance review

5.1 An effective fraud prevention strategy



01

Layered verification

Isolated security checks are no longer sufficient. Organisations must integrate document verification, biometric checks, device fingerprinting, and behavioural analytics across multiple user touchpoints. This multi-layered approach ensures a frictionless experience for legitimate users while deploying dynamic, risk-based defences against fraudsters.



02

AI-driven fraud detection

Machine learning efficiently processes large-scale data to filter out irrelevant signals. Deploying AI enables organisations to reduce false positives, detect complex behavioural patterns, and evaluate anomalies across markets and sectors instantaneously—delivering swift, precise, and scalable decision-making.



03

Behavioural analytics

Identity verification at onboarding only protects the point of entry, whereas fraudulent activity occurs throughout the user lifecycle. Continuous monitoring of behavioural telemetry—including typing dynamics, navigation habits, and abnormal transaction traits—enables systems to catch post-onboarding threats that bypass front-line controls.



04

Global intelligence sharing

Fraud operates across borders, requiring a collective defence strategy. Organisations can fortify their ecosystems by integrating consortium data, shared threat intelligence, and collaborative watchlists. By analysing fraud trends occurring in other sectors or regions, platforms can pre-emptively identify and mitigate emerging threats before impact.

5.2 Education and awareness

Across Southeast Asia, digital literacy is often equated with general awareness, but knowledge alone does not always translate into safer behaviour. Individuals may recognise that scams exist, yet still fall victim due to overconfidence, routine digital habits, or limited exposure to real-world scam tactics.

70%

of scam victims in Malaysia never report their case, pointing to fear and stigma as well as a broader lack of preparedness and accessible support.[35]

Campaigns must go beyond raising awareness to changing behaviours[36]

Educational content must be immersive, locally tailored, and reinforced through schools, workplaces, community programs, and public outreach. Simulation exercises and interactive tools can further build confidence and readiness in daily life. They should help people build digital reflexes such as:

Pause	**Verify**	**Report**	**Practise**
before clicking	digital identities	suspicious activity	through simulation

The box below details a case study on **SGScamWISE**.

In action

Singapore's SGScamWISE

SG ScamWISE (Well-Informed, Secured and Empowered) is a national education programme in Singapore that aims to equip individuals with the skills necessary to protect themselves from scams and fraud. Initiated by Bamboo Builders and supported by Google.org, the initiative reflects a whole-of-society approach to scam prevention.[37]

Rather than relying solely on information campaigns, SG ScamWISE incorporates interactive learning methods aimed at helping participants recognise scam tactics and make safer decisions in real-world situations. The programme combines educational content with practical scenarios and gamified learning experiences, reflecting a broader shift towards behavioural approaches to scam prevention.[38]

The initiative also demonstrates how anti-scam education can be delivered through multiple community touchpoints. Programme activities have been extended to workplaces, schools, community organisations, and social networks, enabling scam awareness messages to reach different demographic groups through channels that are familiar and accessible to them.[39]

As of 2025, the programme had engaged 382 organisations and more than 75,000 individuals. Recent developments include the introduction of gamified learning tools, train-the-trainer programmes and student-focused awareness initiatives, illustrating how scam education efforts continue to evolve alongside changing scam typologies and audience needs. [40]

[35] 37 Billion Reasons the Citizens of Malaysia, Taiwan, and Thailand Need Better Scam Protection, Global Anti-Scam Alliance, 25 September 2024.
[36] Stop raising awareness already, Stanford Social Innovation Review, 2017.
[37] Strengthening online safety in Singapore by educating on AI-powered scams and online threats, Google Public Policy.
[38] SG ScamWISE, Bamboo Builders.
[39] Ibid.
[40] Annual Report 2025, Bamboo Builders, 2025.

5.2 Education and awareness

Singapore Government initiatives for the public

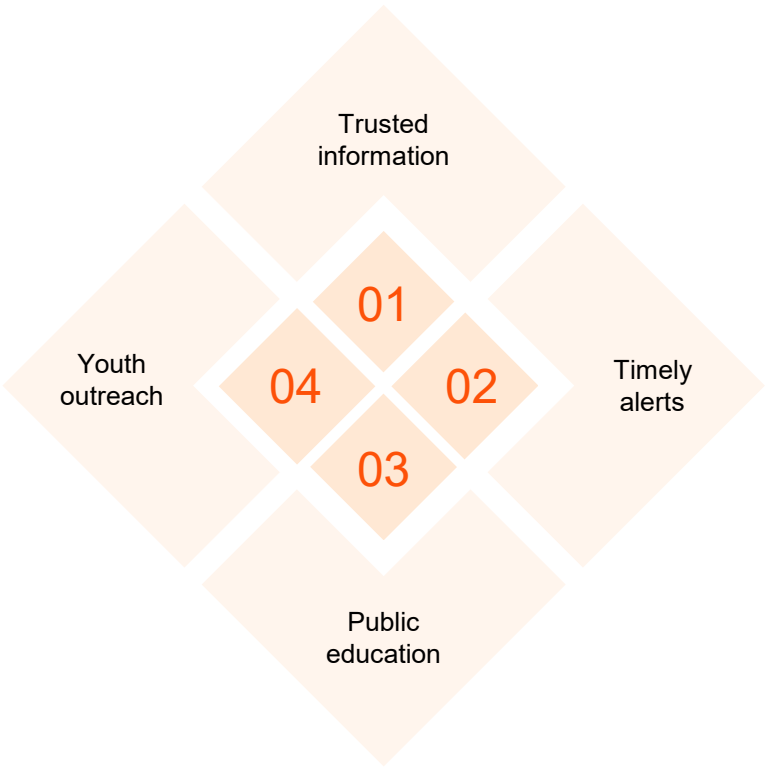
Alongside industry and community-led awareness efforts, the Singapore Government has introduced a range of public-facing initiatives to raise scam awareness and encourage safer digital behaviours. These initiatives provide the public with accessible scam information, timely alerts, educational resources, and youth-focused outreach, while promoting early reporting of suspicious activity.

ScamShield Portal

A national one-stop portal for scam awareness and protection, bringing together scam information, trend updates, prevention guidance, and support resources.[41]

Youth Against Scams

A youth-focused video competition that enables students to create relatable anti-scam content for their peers and amplify awareness through social media networks.[44]



ScamShield Alert Telegram channel

Social channels, including Telegram, extend timely warnings on current scam threats and make alerts easier to share across personal and community networks.[42]

Singapore Police Force (SPF) public awareness campaigns

Scam advisories, trend updates and educational resources help the public recognise common scam methods and take practical steps to protect themselves and others.[43]

From awareness to action

Together, these initiatives support safer digital habits, faster verification and earlier reporting of suspicious activity.

[41] ScamShield Portal, ScamShield.
[42] Launch of ScamShield Suite of Resources, Singapore Police Force, 27 September 2024.
[43] Information on Scams, Singapore Police Force.
[44] Youth Against Scams 2026, Singapore Police Force.

5.3 Assurance and compliance review

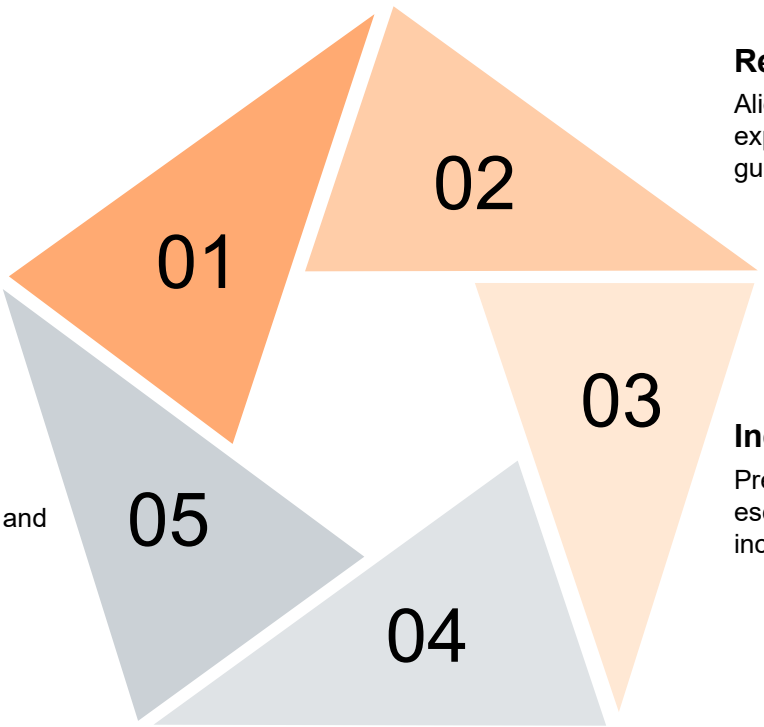
The effectiveness of an anti-scam framework ultimately depends on more than technology deployment or policy implementation. As scam threats continue to evolve, organisations should periodically evaluate whether existing controls remain effective, responsive, and aligned with regulatory expectations.

Assurance reviews provide a structured mechanism to assess key components of an anti-scam framework, from fraud detection controls and incident response processes to governance, oversight, and customer protection measures.

By identifying weaknesses and areas for enhancement, organisations can strengthen their ability to respond to emerging threats while maintaining trust and confidence among customers and stakeholders.

Five domains of anti-scam assurance

A structured view of where controls are effective and where remediation is required



Fraud controls

Effectiveness of fraud detection and prevention measures

Regulatory compliance

Alignment with regulatory expectations and industry guidance

Governance and oversight

Accountability, monitoring and continuous improvement

Incident response

Preparedness to detect, escalate and respond to scam incidents

Fund recovery

Processes supporting investigations and customer remediation

Conclusion



Conclusion



Scams and fraud have become a significant challenge for consumers, businesses and institutions across Singapore and ASEAN

The report in summary

As highlighted throughout this report, scam activity has expanded beyond traditional deception into a broader ecosystem involving digital platforms, payment channels, organised criminal networks, emerging technologies, and cross-border financial flows. While digitalisation has created new opportunities for economic growth and financial inclusion, it has also provided fraudsters with greater scale, reach, and sophistication.

For consumers, this means facing increasingly convincing scams that exploit both technology and human behaviour. For FIs and payment service providers, scams create growing operational, regulatory, and reputational challenges, requiring stronger controls, enhanced monitoring capabilities, and effective customer protection measures. For regulators, law enforcement agencies, telecommunications providers, and digital platforms, the challenge lies in balancing innovation and convenience with the need to disrupt and prevent scam-related harm.

Scam prevention is no longer solely a matter of fraud, compliance, or consumer protection. Increasingly, it sits at the intersection of digital trust, identity verification, customer behaviour, digital assets, and ecosystem accountability. As fraudsters leverage emerging technologies to scale and personalise attacks, organisations need to shift from responding to individual scam incidents towards building resilience across the entire customer journey. This requires not only stronger controls and technologies, but also greater coordination between industry participants, regulators, and consumers to address vulnerabilities that no single stakeholder can resolve alone.

Ultimately, resilience is not defined by the ability to prevent every scam, but by how effectively consumers, organisations, and authorities can anticipate, adapt and respond to an increasingly complex threat landscape. The question is: are we collectively building the resilience needed to prevent, detect and recover from the next generation of scam threats?

About us

At PwC, we help clients build trust and reinvent so they can turn complexity into competitive advantage. We're a tech-forward, people-empowered network with more than 364,000 people in 136 countries and 137 territories. Across audit and assurance, tax and legal, deals and consulting, we help clients build, accelerate, and sustain momentum.

Find out more at https://www.pwc.com/sg/en.html

Sumsub is the first AI-powered trust infrastructure for compliance operations at scale. It connects identity and business verification, fraud prevention, transaction monitoring, and risk workflows, helping teams reduce manual work and enter new markets.

Trusted by over 4,000 clients across financial services, crypto, mobility, trading, marketplaces, education, and iGaming, including Bybit, Bitpanda, Wirex, Avis, Vodafone, Duolingo, Kaizen Gaming, and Bancaribe.

Learn more at https://sumsub.com/

The SFA is a cross-industry non-profit organisation. Its purpose is to support the development of the FinTech industry in Singapore and facilitate collaboration among the participants and stakeholders. The SFA is a member-based organisation with over 600+ members. It represents the full range of stakeholders in the FinTech industry, from early-stage innovative companies to large financial players and service providers. To further its purpose, the SFA also partners with institutions and associations from Singapore and globally to cooperate on initiatives relating to the FinTech industry. Well-connected globally, the SFA has signed over 70 international Memorandum of Understanding (MoU) to lay the network for its members and ecosystem.

For more information visit https://singaporefintech.org/

Connect with us

Wong Wanyi
Partner
FinTech Leader
PwC Singapore
wanyi.wong@pwc.com

Oei Yung Han
Senior Manager
Digital Assets and Payments
PwC Singapore
yung.han.oei@pwc.com

Holly Fang
President
Singapore FinTech Association
holly.fang@singaporefintech.org

Penny Chai
Vice President of APAC
Sumsub
penny.chai@sumsub.com

Jason Chan
APAC Government Relations Lead
Sumsub
jason.chan@sumsub.com

Thank you

© 2026 PwC. All rights reserved. PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

pwc.com