GSMA Intelligence

Towards a digital nation: addressing the scam economy in Asia Pacific

March 2025

The GSMA is a global organisation unifying the mobile ecosystem to discover, develop and deliver innovation foundational to positive business environments and societal change. Our vision is to unlock the full power of connectivity so that people, industry and society thrive. Representing mobile operators and organisations across the mobile ecosystem and adjacent industries, the GSMA delivers for its members across three broad pillars: Connectivity for Good, Industry Services and Solutions, and Outreach. This activity includes advancing policy, tackling today's biggest societal challenges, underpinning the technology and interoperability that make mobile work, and providing the world's largest platform to convene the mobile ecosystem at the MWC and M360 series of events.

We invite you to find out more at gsma.com

GSMA Intelligence is the definitive source of global mobile operator data, analysis and forecasts, and publisher of authoritative industry reports and research. Our data covers every operator group, network and MVNO in every country worldwide – from Afghanistan to Zimbabwe. It is the most accurate and complete set of industry metrics available, comprising tens of millions of individual data points, updated daily.

GSMA Intelligence is relied on by leading operators, vendors, regulators, financial institutions and third-party industry players, to support strategic decision-making and long-term investment planning. The data is used as an industry reference point and is frequently cited by the media and by the industry itself.

Our team of analysts and experts produce regular thought-leading research reports across a range of industry topics.

www.gsmaintelligence.com

info@gsmaintelligence.com

Author

Kenechi Okeleke, Senior Director, GSMA Intelligence

Contributors

Jeanette Whyte, Head of Policy & External Affairs, Asia Pacific
Syed Khairulazrin Bin Syed Khairuldin, Policy Director, Asia Pacific
Ming Sheng Bensen Koh, Senior Policy Manager, Southeast Asia

Contents

Executive summary

Scams continue to grow in reach, sophistication and impact

The rapid expansion of digital technologies, and mobile connectivity in particular, has profoundly impacted scam techniques and their reach. All individuals with a mobile subscription – approximately 5.8 billion people – are potential targets for scams. Rises in the volume, frequency, sophistication and success rate of scams in recent years are having a significant financial impact on victims and the global economy. According to the 2024 Global State of Scams report by the Global Anti-Scam Alliance (GASA), scammers siphoned more than $1.03 trillion worldwide over the past year.[1] The increasing incidence of scams and their associated financial consequences are commonly referred to as the ‘scam economy’.

The ecosystem builds on efforts to combat scams

Key stakeholders, including governments, mobile operators, digital platforms and payment service providers, have focused on addressing the scam economy. This builds on growing recognition of the importance of maintaining trust in the digital ecosystem. It requires a shift from assigning blame for fraudulent activities to using collaborative mechanisms to effectively combat scams. The GSMA Open Gateway initiative aims to harness the capabilities of mobile networks worldwide by providing access through standardised APIs. It provides a platform for mobile operators to tackle scams directly and serve enterprises with anti-fraud solutions. As of February 2025, 72 operator groups, representing 284 networks and accounting for 78.5% of mobile connections, had committed to the initiative.

Preserving trust in the digital world will remain a priority for governments, operators and other stakeholders. This is essential to sustain the growth of digital services and their contribution to socioeconomic progress, in line with the digital ambitions of governments across Asia Pacific. Addressing the scam economy is crucial to achieving this goal, given the erosive effect that online scams and fraudulent activities can have on public trust.

As stakeholders build on efforts to address the scam economy, several considerations will be top of mind. This report highlights six considerations: the role of AI and other emerging technologies in addressing scams; opportunities for monetising anti-scam solutions; ecosystem-wide collaboration to combat scams; secure digital transformation initiatives; a collaborative approach to addressing cross-border scams; post-fraud support for victims; and privacy and ethical considerations.

[1] Global State of Scams Report, 2024, Global Anti-Scam Alliance, 2024

A collaborative framework is essential to preserve trust in the digital environment

The digital ecosystem has a unique opportunity to combat the scam economy through collaborative efforts. Participants in the digital ecosystem, particularly operators and digital platforms, should articulate the positive outcomes of collective actions to address the scam economy. This can be achieved by documenting and sharing instances where joint initiatives have successfully prevented scams, and by highlighting the tangible benefits of cross-ecosystem collaboration.

There is no better time than now to adopt a unified, ecosystem-wide approach to fighting scams to accelerate progress and counter emerging threats. By integrating diverse expertise and perspectives, and working within a collaborative framework, the digital ecosystem is well placed to lead efforts to preserve trust in the digital environment.

1. The scam economy in context

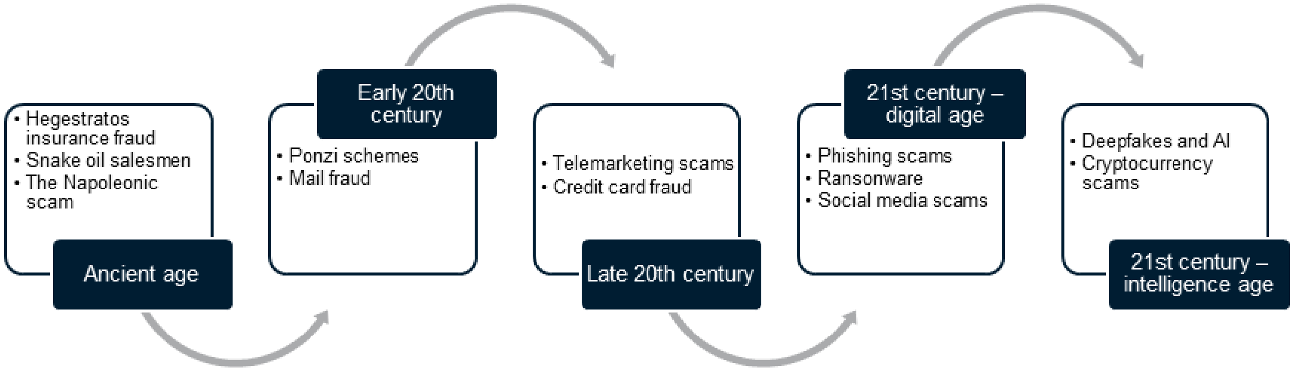
The evolution of scamming methods

Scams have been a part of human interaction throughout history. While the underlying principles and motivations behind scams have remained consistent across generations and cultures, the methods have evolved in response to societal changes.

Since the 20th century, technological advancements have significantly influenced the evolution of scamming methods. This has seen a transition from simple, physical tactics, such as sinking cargo ships for insurance claims, to sophisticated scams employing digital technologies (see Figure 1). Over the past three decades, the rapid expansion of digital technologies, particularly mobile connectivity, has profoundly impacted scam techniques and their reach. Today, all individuals with a mobile subscription – approximately 5.8 billion people, including 4.7 billion who also use mobile internet – are potential targets for scams. This figure increases considerably when accounting for individuals without a mobile subscription but who have regular access to the internet or a mobile connection via other means, such as through a friend or relative.

Figure 1: Examples of scam methods over time

Source: GSMA Intelligence



Ancient age
- Hegestratos insurance fraud
- Snake oil salesmen
- The Napoleonic scam

Early 20th century
- Ponzi schemes
- Mail fraud

Late 20th century
- Telemarketing scams
- Credit card fraud

21st century – digital age
- Phishing scams
- Ransomware
- Social media scams

21st century – intelligence age
- Deepfakes and AI
- Cryptocurrency scams

The attraction of the digital environment

Various factors make the digital environment attractive to scammers, including the following:

- **Anonymity** – The internet enables users to operate behind false identities, spoofed emails or encrypted platforms, making it more challenging for authorities to trace their activities than in the physical world.

- **Scale** – The internet allows individuals to reach a large number of people worldwide with minimal effort. For instance, phishing emails can be distributed to numerous addresses rapidly, while offline scams such as door-to-door fraud require more time and are limited to a local area.

- **Cost** – Online scams are typically less expensive to carry out. For instance, creating a fraudulent website or sending mass messages usually costs less than producing fake flyers or organising a physical setup.

- **Digitalisation** – As digital platforms are increasingly used for daily transactions, certain practices (such as social media oversharing and inadequate data security) provide scammers with access to individuals' personal data and financial assets. This increases vulnerabilities and allows scammers to tailor their attacks more effectively.

- **Enforcement** – Scammers can target victims on a global scale, circumventing local law enforcement and exploiting legal loopholes in various jurisdictions. Offline scams are typically confined to a single jurisdiction, which allows authorities to more easily track perpetrators.

- **Trust exploitation** – Regular use of the internet conditions individuals to perform actions such as clicking links or opening attachments in emails that appear to be from legitimate sources. Scammers exploit these habits through social engineering tactics and other methods to disguise their deception.

- **Technology evolution** – The rapid advancement of technology enables scammers to enhance the complexity of their schemes, such as through the creation of deepfakes. Awareness and legislative measures often lag behind innovations, creating opportunities for scammers to exploit.

The expanding range of scam activities

Online scams and fraud can take various forms. Common examples include the following:

- **Authorised push payment (APP) fraud** – Someone is deceived into sending money to a fraudster posing as a genuine payee from a trusted organisation, such as a bank.

- **Baiting –** Criminals offer something enticing, such as free software downloads, in exchange for personal information or system access. This can involve infected digital files or links.

- **Business email compromise** – Criminals gain access to a business's email system and deceive employees into disclosing confidential information or transferring money.

- **Identity fraud** – A form of impersonation that involves taking over a genuine identity of another or creating a fictitious one.

- **Identity theft** – Theft of an individual's personal information to commit fraud. Perpetrators typically obtain personal information or documents such as identity numbers or cards, biometrics or passwords, and use them to assume the identity of others.

- **Impersonation** – Criminals pretend to be someone else (online, over the phone or in person) to gain trust and manipulate a victim into disclosing confidential information or taking specific actions.

- **Phishing** – Deceptive emails, messages (including SMS), social media or links to websites appear legitimate, aiming to trick recipients into clicking and revealing sensitive information such as passwords, credit card numbers or other personal data. This often involves impersonation, where criminals pretend to be a trustworthy entity, such as a bank, government agency or employer.

- **Pretexting** – Criminals create a fabricated scenario or pretext to obtain information. This often involves impersonating someone trustworthy, such as a colleague or bank representative.

- **SIM swap fraud** – A fraudster tricks a mobile service provider into porting or transferring a victim's mobile phone number to a new SIM card under the fraudster's control.

- **Smishing (SMS) and vishing (voice calls)** – Criminals impersonate trusted entities and persuade victims to reveal sensitive information such as passwords, credit card numbers or other personal data. This often involves impersonation, where the criminal pretends to be a trustworthy entity, such as a bank, government agency or employer.

- **Spoofing** – Attackers manipulate online information, such as email addresses or contact names/numbers, to falsely represent their identity.

In addition to the above, the 'pig butchering' scam has become prevalent in Asia Pacific. This is a long-term scam that combines romance and investment fraud. A victim is gradually lured into investing in a fraudulent cryptocurrency scheme, ultimately leading to the theft of their assets. These operations also involve human trafficking, with a UN report estimating that at least 120,000 people across Myanmar and around 100,000 in Cambodia may be trapped in scam operations, with other criminal-owned enterprises in Laos, the Philippines and Thailand ranging from crypto-fraud to online gambling.[2] Recent reports indicate that Chinese, Thai and Myanmar authorities are cooperating in efforts to dismantle scam centres and illegal online operations along their borders. These collaborative actions have led to the rescue of several thousand individuals who were trafficked into working in these centres.[3]

While these and other tactics have existed since the advent of the digital age, they have been significantly enhanced by artificial intelligence (AI). Scammers now leverage AI tools, including generative AI (genAI), to execute highly sophisticated attacks that are more challenging to detect or mitigate. Common AI-enabled scams include:

- deepfakes **–** using AI to create realistic fake videos and audio clips to impersonate celebrities, executives or even friends and family members

- personalisation – using AI to generate highly personalised phishing and smishing messages that are difficult to distinguish from legitimate ones

- automated social engineering – using AI to analyse social media profiles and other online data to craft convincing messages that exploit personal details.

Between 2022 and 2023, Asia Pacific experienced a 1,530% increase in deepfake fraud. Countries including Malaysia, Singapore and Indonesia have issued warnings about these high-tech scams, which use manipulated videos and audio to deceive victims.[4]

The impact on victims

Rises in the volume, sophistication, frequency and success rate of scams in recent years are having a significant financial impact on victims and the global economy. According to the 2024 Global State of Scams report by the Global Anti-Scam Alliance (GASA), scammers siphoned more than $1.03 trillion worldwide over the past year.[5] The report highlights that individuals in the US experienced the highest losses, with an average of $3,520 per victim. Countries in Asia Pacific are also facing substantial economic costs due to fraudulent activities. For example, in India, more than INR11,000 crore ($1.5 billion) was lost to online scams during the first nine months of 2024, with stock trading and investment scams the most frequently reported cases.[6] In Thailand, the Anti-Online Scam Operation Centre recorded five significant scam cases within one week in January 2025, resulting in a total loss of THB21 million ($610,000).[7]

[2] Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape, UNODC, 2024
[3] "Thousands in limbo on Thai-Myanmar border after scam centre crackdown", Bangkok Post, February 2025
[4] "Cyber Scamming Goes Global: Unveiling Southeast Asia's High-Tech Fraud Factories", CSIS, December 2024
[5] Global State of Scams Report, 2024, Global Anti-Scam Alliance, 2024
[6] "India lost over INR11,000 crore to cyber scams in first 9 months of 2024: Report," Hindustan Times, November 2024
[7] "Thailand: Online Safety Awareness and Cybersecurity Efforts", OpenGovAsia, January 2025

The increasing incidence of scams and their associated financial consequences are commonly referred to as the ‘scam economy’. While there is no formal definition for this term, it typically describes a system where fraudulent activities, deception and exploitation generate economic activity. It also encompasses the ecosystem of scams: the perpetrators, the tools they use, the victims they target and the funds extracted. The ‘scam economy’ focuses on the deception and exploitation of individuals; it is a subset of the ‘fraud economy’. The latter comprises all types of fraudulent activities, including those affecting businesses and institutions. Although these terms are sometimes used interchangeably, this analysis focuses on the impact on individuals.

2. The impact of the scam economy

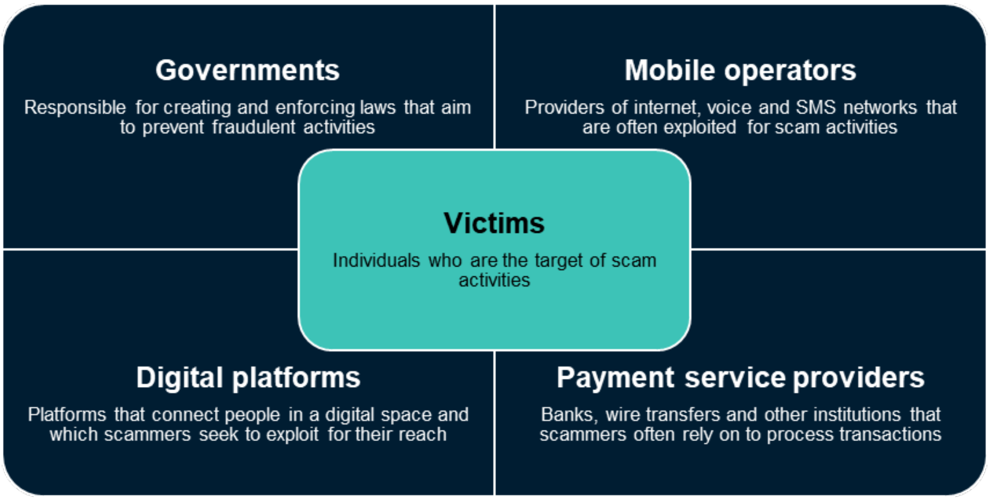
The scam economy involves various unwilling stakeholders in its operations. These are individuals and entities indirectly affected by fraudulent activities, often without their knowledge or consent. They are vulnerable to the negative impacts of the activities.

A major impact of scams, which affects the whole of society, is the reduction of trust in digital platforms. This occurs when the confidence that people place in systems, institutions and each other is compromised due to scams. It has the potential to disrupt the ambitions of governments and their private sector partners to build inclusive digital nations.

A first step to addressing fraudulent activities in the economy is to identify the roles of individuals and entities (Figure 2) often entangled in the scams, and how they are impacted by the activities.

Figure 2: Individuals and entities entangled in the scam economy

Source: GSMA Intelligence



Governments

Responsible for creating and enforcing laws that aim to prevent fraudulent activities

Mobile operators

Providers of internet, voice and SMS networks that are often exploited for scam activities

Victims

Individuals who are the target of scam activities

Digital platforms

Platforms that connect people in a digital space and which scammers seek to exploit for their reach

Payment service providers

Banks, wire transfers and other institutions that scammers often rely on to process transactions

Victims

Every scam unfortunately involves a victim. These are often individuals who lose personal information and financial assets to scammers. They can also include entities targeted through tactics such as invoice scams or data breaches, which then expose their customers to personal scams. Scammers use social engineering tactics to exploit trust, ignorance, greed, desperation or a combination of these vulnerabilities to deceive victims into providing personal information, money or access to valuable assets.

The financial impact of scams on victims is typically the most evident because it is quantifiable. However, the effects extend beyond monetary loss, often including significant psychological consequences, such as feelings of shame, shock, anger, frustration and anxiety, among other negative emotions. Additionally, if a stolen identity is used for fraudulent activities, scams can lead to reputational damage for the victims.

Governments

Governments and policymakers assume a complex role in combating scams, encompassing prevention, enforcement and damage control to protect citizens, uphold trust in digital systems, and deter fraudulent activities. Primarily, governments establish the legal frameworks that define scams and determine penalties for perpetrators and any stakeholders who fail in their duties to prevent such crimes.

Cross-border scams pose a substantial challenge due to the high costs involved and the necessity for cooperation with authorities across different jurisdictions. For instance, the United Nations estimates that hundreds of thousands of individuals have been trafficked to work as online scammers in various Southeast Asian countries, including Cambodia, Laos and Myanmar, targeting victims throughout Asia Pacific and beyond.[8]

Governments themselves are vulnerable to fraud schemes that exploit their systems, resources or authority without proper consent or awareness. For instance, scammers may use counterfeit government-branded emails or websites to deceive individuals into disclosing personal information or making payments. Such scams can have substantial economic and social repercussions for the government, including lost revenue due to tax evasion and diminished public trust in government systems.

According to a report by the Singapore Police Force, impersonation scams targeting government officials resulted in the highest average losses, approximately $116,534 per case during the first half of 2024.[9] In the Philippines, the Bureau of Immigration warned the public about scammers running fake websites charging for e-travel registration. Similarly, New Zealand's Inland Revenue Department in 2024 highlighted a convincing email scam targeting those awaiting tax refunds.

Mobile operators

Mobile operators often find their services, such as voice calls, SMS and internet connectivity, exploited by scammers to reach victims. Activities include spoofing, phishing and smishing via mobile networks. In 2024, caller ID and scam prevention app Whoscall detected 168 million scam calls and SMS messages in Thailand, representing a 112% increase from 79.2 million in 2023 – the highest figure in five years.[10] Scams negatively impact the financial performance, reputation and operational efficiency of operators. For instance, operators often bear the brunt of unpaid bills, unauthorised usage and stolen services. Operators may also face additional regulatory action such as fines.

[8] “Hundreds of thousands trafficked to work as online scammers in SE Asia, says UN report”, UN, August 2023

[9] Mid-Year Scams and Cybercrime Brief 2024, Singapore Police Force

[10] "Whoscall reveals 2024 statistics: scam calls and SMS surge to 168 million", The Nation Thailand, February 2025

Operators must balance security and privacy considerations, and are legally required to protect the confidentiality of communications and user privacy. This can limit their ability to filter or block network traffic without risking the disconnection of legitimate users.

Operators devote significant resources to scam prevention, detection and mitigation solutions. This includes investing in technical solutions, increasing customer-service staff to manage complaints, and working with regulators or law enforcement to identify perpetrators. In India, operators have been required to implement awareness campaigns and enhance network security in response to widespread know-your-customer (KYC) and one-time password (OTP) scams, where fraudsters deceive users into disclosing credentials through calls or SMS. In Indonesia, operators have made substantial investments in fraud management systems. These investments potentially divert resources away from growth initiatives.

Digital platforms

Digital platforms are online frameworks or environments that facilitate the exchange of information, services or goods between users. They generally fall into the following categories:

- social media platforms – websites and apps that allow users to create, share and interact with content, such as Facebook, X (formerly Twitter) and Instagram

- e-commerce platforms – online marketplaces where users can buy and sell products, such as Amazon, eBay and Alibaba

- content platforms – services that provide access to various forms of digital content, including videos, music and articles, such as YouTube, TikTok and Spotify

- communication platforms – tools that enable users to communicate and collaborate in real-time, such as Zoom, Slack and Microsoft Teams

- service platforms – websites and apps that connect users with service providers, such as Uber, Airbnb and TaskRabbit.

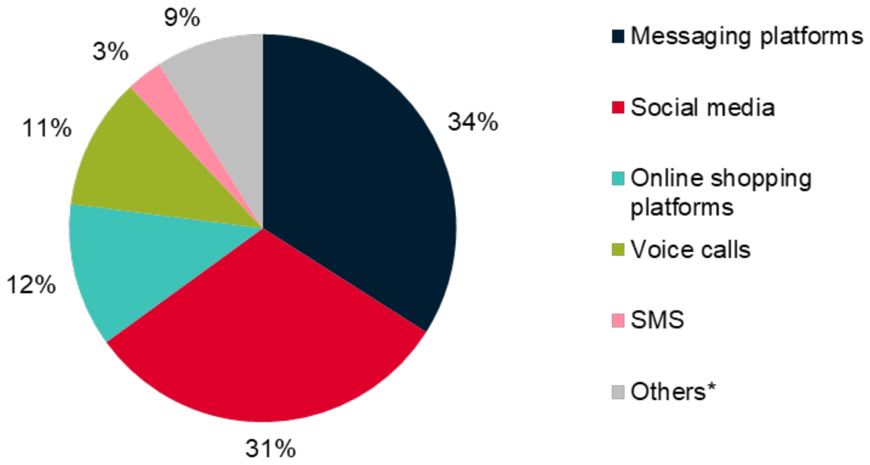
Digital platforms are designed to enable connection, engagement and commerce. However, their expansive scale, extensive reach and open nature make them attractive targets for scammers aiming to exploit users. Several factors contribute to this vulnerability: a large user base that offers a broad pool of potential victims; low barriers to entry that allow scammers to easily establish accounts; anonymity that enables the creation of fake profiles or the use of pseudonyms; and the capability for rapid communication, allowing scammers to swiftly contact numerous individuals.

The social media business model relies on user autonomy and minimal barriers to entry, facilitating easy registration, posting and advertising. However, this model is often exploited by scammers who employ various methods such as creating fake accounts, distributing phishing links and placing fraudulent advertisements. Additionally, digital platforms with extensive user bases provide scammers with a vast pool of potential victims and tools, such as direct messaging, to reach them.

According to figures published by the platforms themselves, Facebook had the highest number of monthly active users (3.07 billion) as of February 2025. Other platforms in the top five include YouTube (2.53 billion), WhatsApp (2 billion), Instagram (2 billion) and TikTok (1.5 billion).

In Singapore, data from authorities indicates that messaging and social media platforms accounted for 34% and 31%, respectively, of reported scam cases during the first half of 2024, compared to 11% and 3% for voice and SMS (see Figure 3). For social media and other digital platform providers, the challenge involves balancing user experience and privacy with the implementation of stricter measures to make platforms less appealing to scammers. Although it can be a complex task, it is necessary for maintaining trust and safety around digital platforms.

Figure 3: Singapore – breakdown of reported scam cases by contact method
Source: Singapore Police Force



*Dating apps/websites, emails, classified ads and online streaming services.

Scams affect the finances, reputation and operational efficiency of digital platforms. Financially, digital platforms may face backlash from advertisers concerned about scams, as well as legal and regulatory costs from lawsuits by victims or regulators seeking accountability. Scams can deter legitimate users and businesses, reducing the active base that generates ad revenue and network effects. This is directly related to the reputational impact for a digital platform perceived to have a high incidence of fraudulent activities. Scams also require significant resources to combat them. For example, companies such as Google and Meta have reported substantial investments in AI systems to address scams and other fraudulent activities.

Payment service providers

Payment service providers (PSPs) and banks are sometimes entangled in scams, as they are part of the financial system that scammers use to move money and deceive victims. Scammers use PSP services to conduct transactions through various methods, such as fake online purchases, phishing schemes or money laundering. For example, a fraudster may trick an individual into sending money using a payment app or wire transfer – and the bank or provider processes that transaction without being aware of its fraudulent nature. A 2023 report from the Federal Trade

Commission in the US indicated more than $10 billion in fraud losses, much of it occurring through legitimate financial channels.[11] PSPs and banks face the challenge of releasing customer funds on request while also protecting them from potential scams.

Growing adoption of digital payments has made them a prime target for fraudsters. For instance, mobile devices are implicated in 74% of global digital payment fraud incidents, reflecting the shift to mobile-first transactions. Furthermore, peer-to-peer payment platforms have witnessed an 80% increase in fraud incidents as their popularity rises, often without adequate security measures[12] – a situation that is increasingly attracting the attention of regulators. In January 2025, the Consumer Financial Protection Bureau (CFPB) ordered Block, the operator of the peer-to-peer payments app Cash App, to issue refunds and other redress to consumers totalling up to $120 million and a penalty of $55 million to be paid into the CFPB's victims relief fund. The order was due to security protocols for Cash App deemed insufficient by the CFPB, which exposed its users to potential risks of fraud.[13]

PSPs and banks frequently refund victims, at least partially, either due to legal obligations or to maintain customer loyalty. In January 2025, the Bank of Thailand mandated that all banks expedite refunds for victims of credit card fraud, ensuring compensation within five business days if the cardholder is found not to be responsible. In December 2024, Malaysia Prime Minister Anwar Ibrahim advocated for a policy similar to that of the UK, where banks are required to reimburse scam victims. As of the time of writing, this policy was still under review, but it signifies a growing trend towards holding financial institutions accountable.

[11] "As Nationwide Fraud Losses Top $10 Billion in 2023, FTC Steps Up Efforts to Protect the Public", FTC, February 2024
[12] See www.coinlaw.io/digital-payment-fraud-statistics
[13] "CFPB Orders Operator of Cash App to Pay $175 Million and Fix Its Failures on Fraud", Consumer Financial Protection Bureau, January 2025

3. Addressing the scam economy

A secure and reliable digital environment promotes increased participation in online transactions by individuals and businesses, contributing to economic growth and innovation. Stakeholders have consequently focused on addressing the scam economy in recent years. At the organisational level, efforts are largely driven by strategies to reduce the financial, reputational and operational impacts of scams. Additionally, there is growing recognition among stakeholders of the importance of maintaining trust in the digital ecosystem. This requires a shift from assigning blame for fraudulent activities to using collaborative mechanisms to effectively combat scams.

Government-led efforts

Governments and regulators in Asia Pacific and beyond are increasing efforts to combat scams through enforcement, industry collaboration and public education.

A whole-of-government approach (WGA)

This strategy entails addressing the scam economy through comprehensive cross-agency collaboration with industry stakeholders. The objective is to streamline efforts and enhance efficiencies in formulating and implementing government prevention and enforcement mechanisms. Additionally, it ensures that the concerns of various stakeholders are considered for the effective allocation of resources.

For example, in July 2023, the Australian government established the National Anti-Scam Centre (NASC) within the Australian Competition and Consumer Commission (ACCC). The NASC aims to foster collaborative efforts among government agencies, law enforcement, consumer organisations and industry stakeholders, including financial service providers, operators and digital platforms, to combat scams. The NASC has been credited with contributing to a 13.1% reduction in reported losses in Australia during 2023.[14]

Legislation

This establishes a structured and enforceable framework to safeguard citizens from fraudulent activities. It does so by delineating explicit rules to identify scams, imposing penalties on perpetrators and defining the responsibilities of various stakeholders. Additionally, legislation often includes provisions for victims to seek redress, and mandates the creation or designation of an organisation to ensure compliance.

For example, in February 2025, Australia passed the Scams Prevention Framework Bill. The Australian Communications and Media Authority and other regulators will enforce industry codes for banks, telecoms operators and social media firms. Operators must block scam SMS and calls,

[14] "Scam losses decline, but more work to do as Australians lose $2.7 billion", ACCC, April 2024

and social media firms must verify advertisers. The framework is to become fully active by mid-2025.

In January 2025, it was reported that the Malaysian government was reviewing proposals to amend digital-related laws to regulate social media platforms and address online scams and fraud. The proposed amendments would expand the scope of responsibility to include telecoms operators, with coordination led by Bank Negara Malaysia.

While swift regulatory action is crucial to addressing digital fraud, rushing the creation and implementation of new legislation carries potential risks. Poorly designed laws, which are not technology-neutral and often lag behind technological innovation, are often exploited by bad actors. There are also unintended consequences, such as overly broad enforcement measures that stifle legitimate digital services, increased compliance costs for businesses, or gaps in regulatory oversight that could be exploited by bad actors.

Regulatory actions

Regulatory authorities overseeing critical sectors, such as telecoms or financial services, issue standards and guidelines for stakeholders to aid in the prevention, detection and penalisation of fraudulent activities. These measures are intended to ensure stakeholders implement comprehensive security protocols to safeguard consumers from scams.

- In February 2025, the Securities and Exchange Board of India issued a consultation paper proposing more stringent KYC regulations. These include the mandatory linking of SIM cards and biometric verification, along with real-time monitoring for financial platforms, to combat investment scams such as fraudulent trading applications.

- In December 2024, the Department of Telecommunications in India announced the deactivation of more than 8.5 million mobile connections that were either registered with fake documents or linked to fraudulent activities. This action followed the introduction of ASTR – an AI-powered facial recognition tool that aids in detecting SIM cards obtained under multiple names by the same individual.

- In January 2023, Singapore implemented the Singapore SMS Sender ID Registry (SSIR) and the Decision on the Implementation of Anti-Scam Filter Solutions within mobile networks. These require organisations that use SMS Sender IDs to register with the SSIR maintained by the Infocomm Media Development Authority (IMDA), and operators to implement systems that scan all SMS messages to cross-check URLs against a continuously updated database of known malicious links. In December 2024, the Monetary Authority of Singapore and IMDA jointly introduced a new Shared Responsibility Framework that assigns banks and operators relevant duties to mitigate phishing scams. Accordingly, banks are implementing tools such as Singpass Face Verification for high-risk transactions, while operators are enhancing SMS sender ID checks, building on the 2023 SSIR mandate.

International cooperation

The cross-border nature of online scams makes it challenging for any single country to address them effectively. International cooperation facilitates the sharing of information, resources and skills to track and prosecute scammers globally. Additionally, by collaborating, countries can combine their efforts to develop more effective anti-scam strategies and harmonise regulations and standards, reducing the opportunities for scammers to exploit regulatory discrepancies between countries. For example, in January 2025, the Commercial Affairs Department of the Singapore Police Force and Commercial Crime Investigation Department of the Royal Malaysia Police jointly dismantled a transnational scam syndicate involved in government official impersonation scams in Malaysia. In December 2024, ACMA in Australia and UK telecoms regulator Ofcom agreed to improve information sharing and cooperation to combat phone scams, spam and unsolicited calls.

Data sharing

This refers to enhancing detection capabilities by identifying patterns and anomalies indicative of fraudulent activities. By pooling data, organisations can develop more effective preventive measures. For instance, the collective intelligence of PSPs, operators and social media platforms can facilitate more accurate and timely scam detection. Examples of government-led data sharing initiatives in Asia Pacific include the following:

- In 2023, the Australian Competition and Consumer Commission (ACCC) initiated the Scam-Safe Accord, aimed at encouraging operators and banks to exchange scam-related data with each other and regulators. This includes information on spoofed numbers, phishing attempts and fraud trends, contributing to a national anti-scam database. The ACCC also collaborates with social media platforms to remove scam content based on shared intelligence.

- The Philippines Anti-Financial Account Scamming Act, enacted in 2024, enhances data sharing between the Bangko Sentral ng Pilipinas, financial institutions and law enforcement agencies to monitor and freeze accounts associated with scams. Additionally, the Cyber and Forensics Division of the Philippine SEC collaborates with foreign regulators by providing evidence to combat cross-border fraud, including fraudulent loan applications.

- In Singapore, the Anti-Scam Command (ASCom) collaborates with various stakeholders, including financial institutions and telecoms operators, to share data and intelligence on scam activities. This facilitates the prompt detection and disruption of scam operations. ASCom aims to achieve greater synergy between the various scam-fighting units within the Singapore Police Force.

- At the 42nd Association of Southeast Asian Nations (ASEAN) Summit in May 2023, leaders committed to strengthening cross-border data sharing to combat online scams and human trafficking. The ASEAN Senior Officials Meeting on Transnational Crime plays a key role in facilitating intelligence exchange on scam networks. This often involves collaboration with

Interpol and the United Nations Office on Drugs and Crime, focusing on hubs in Myanmar, Cambodia and Laos.

Awareness campaigns

These initiatives aim to educate individuals on scam tactics and how to protect themselves. They also provide information on tools that can be used to prevent scams and, importantly, guidance on reporting cases and seeking redress. Scammers exploit ignorance; education is a key strategy to combat it. For instance, in January 2025, the Cyber Security Agency of Singapore updated its list of recommended security applications that the public can use to safeguard their devices against malware attacks and phishing attempts. In Malaysia, the Royal Malaysia Police has initiated the Stop Scams campaign, which includes public service announcements, social media campaigns and community engagement activities designed to educate the public on scams and preventive measures.

Mobile operators

Operators are continually improving their efforts to address scams within their networks, as the threat landscape evolves with new technologies. Beyond regulatory-mandated consumer protections, operators also run awareness campaigns and work together and with authorities by sharing actionable intelligence.

Many operators invest in advanced solutions and initiatives that use modern technologies to combat scams, while offering premium opt-in services such as enhanced call-blocking apps or spam filters. These solutions employ AI and machine-learning tools to monitor messages, user behaviour and network activity to detect scam patterns in real-time. They analyse call and SMS traffic for anomalies, such as sudden spikes to premium-rate numbers or spoofed caller IDs, and flag or block them before they reach customers. Table 1 provides examples from countries across Asia Pacific.

Table 1: Examples of advanced fraud detection solutions

Source: GSMA Intelligence

Operator	Solution
Airtel	In September 2024, Airtel introduced a network-based solution that uses AI to detect spam calls and messages in India. It analyses 250 parameters, such as a caller or sender usage patterns, call/SMS frequency and call duration, in real-time. By cross-referencing the information against known spam patterns, the system identifies suspected spam calls and SMS.
Axiata	Axiata has implemented its Helios platform across its operations in Asia Pacific, including Malaysia (CelcomDigi), Indonesia (XL Axiata) and Sri Lanka (Dialog Axiata). The Helios platform conducts real-time analysis to identify and prevent fraudulent activities, such as unauthorised network access and scam attempts, within its networks.
NTT Docomo	NTT Docomo uses an advanced machine-learning system to address subscription fraud and premium-rate scams. Its analytical tools process extensive datasets to identify irregular usage patterns, such as sudden increases in international calls. The system is aligned with Japan’s national initiatives to combat telecoms fraud through improved KYC processes.
SK Telecom	SK Telecom has implemented AI-powered fraud detection, which includes real-time network monitoring and voice biometrics. The systems analyse call data and user behaviour to identify anomalies, such as SIM box fraud or account takeovers. Additionally, SK Telecom's approach incorporates predictive analytics to anticipate AI-enabled deepfake and phishing scams.
Telstra	Telstra has implemented a solution in accordance with Australia’s Reducing Scam Calls Code, using network-level blocking and AI analytics to identify and prevent scam calls, including those using spoofed numbers. In 2024, Telstra reported blocking millions of scam calls in compliance with ACMA regulations. The company employs behavioural analytics to detect unusual traffic patterns indicative of fraud, such as Wangiri or PBX hacking.
True Corporation	In December 2024, True Corporation launched True CyberSafe – a cyber-protection system designed to safeguard against online fraudulent activities in Thailand. This system offers protection from phishing links and scam SMS, and includes call filtering. By the end of January 2025, True Corporation reported that True CyberSafe successfully blocked more than 370 million suspicious link clicks, protecting its customers from potential scams.

Digital platforms

Digital platform providers are addressing scams through a combination of technology tools, policy enforcement and user-education initiatives. Many platforms implement advanced algorithms and AI to detect and eliminate fraudulent accounts, suspicious advertisements and phishing attempts before they reach users. For instance, some companies analyse patterns in account behaviour, such as rapid posting or messaging from newly created profiles, to identify potential scams. They also employ machine learning to detect deceptive content or impersonation attempts. Some companies have introduced verification processes to authenticate accounts claiming to represent legitimate brands or individuals, mitigating impersonation risks.

Several platforms now offer user empowerment tools, including alerts for suspicious accounts, options to report scams directly, and privacy settings that restrict who can contact users or view their information. Additionally, some platforms have introduced features such as call silencing for unknown numbers and warnings on risky links to safeguard users in real time.

Education plays a crucial role in the efforts of digital platform providers to combat scams. Educational initiatives are often delivered through in-app notifications, blog posts or partnerships with consumer protection agencies, aiming to inform users on common tactics such as unsolicited messages from fake profiles.

Table 2 provides examples of the measures taken by digital platform companies.

Table 2: Examples of efforts by digital platform companies to tackle the scam economy

Source: GSMA Intelligence

Digital platform	Solution
Meta	**AI detection and remova**l – Meta employs machine-learning models to identify and eliminate scam content, including fraudulent advertisements for cryptocurrency schemes and counterfeit products. In 2023, Meta reported the annual removal of more than 1.3 billion fake accounts, many associated with scams, by analysing behavioural signals such as mass friend requests and spammy posting patterns. **Phishing prevention –** The system identifies and flags potentially malicious links within messages or posts, providing users with warnings prior to clicking. **User tools –** Instagram's Restricted Accounts feature allows users to limit interactions from specific profiles, while Facebook's Report Ad option lets users flag advertisements for review, including those related to potentially fraudulent promotions.
Google	**Data sharing –** Google collaborated with the Indian Cyber Crime Coordination Centre to integrate Google Pay into the National Cybercrime Reporting Portal, aiding in data sharing for financial fraud investigations. **Ad and comment filters –** YouTube's systems block scam advertisements and remove comments containing phishing links or cryptocurrency scam content. The platform has also implemented stricter policies to demonetise channels that promote fraudulent activities. **User reporting –** Improved reporting tools allow viewers to flag videos as scams, prompting human review when AI confidence is insufficient, particularly for complex fraud such as multilevel marketing presented as lifestyle vlogs. **SMS filters –** Google, the Singapore Police Force and IMDA are collaborating on a pilot opt-in feature that would allow Android users to block SMS from unknown international numbers by adjusting their Protection and Safety settings in Messages. **App filters –** Google Play Protect provides free, real-time scanning of apps from the Google Play Store and Android devices, identifying and removing harmful software while alerting users to potential risks.
TikTok	**Content moderation –** TikTok employs AI to scan videos and comments for indicators of scams, such as 'cash-flipping' promises or pyramid scheme pitches. In its 2023 safety report, TikTok noted that 95% of content violating its policies was removed proactively. **Creator accountability –** The platform enforces strict measures by banning accounts that promote fraudulent side businesses, and collaborates with financial regulators to target investment scams, including those that promote non-existent tokens during live streams. **Educational campaigns –** TikTok conducts in-app warnings, and works with authorities to educate users about various types of scam.
X	**Bot and spam crackdowns –** X uses automated systems to detect and suspend bot accounts frequently involved in scams, such as fake giveaways or impersonating executives. **Verification overhaul –** X has recently revised its verification system (including paid blue ticks and organisational badges) to decrease impersonation scams by making it more challenging for fraudsters to pose as legitimate personalities or brands. **Community Notes –** This user-driven feature allows people to flag misleading posts, including scams such as fake donation drives, adding context that alerts others in real-time.

Despite these efforts, challenges continue as scammers quickly adapt and discover new loopholes to exploit. Additionally, the large volume of traffic, such as billions of social media posts daily on some platforms, makes it difficult to monitor every interaction. Not all fraudulent activity is reported, which suggests the scale of the issue may be greater than what is currently known.

One area that is the subject of debate for social media platforms is the introduction of ID verification for all users. Arguments in favour of this as a tool to combat scams include its potential to make it more challenging for scammers to create fake accounts, its ability to promote a safer and more trustworthy online environment, and the idea that users may be less likely to engage in fraudulent activities if their identities are known. However, opposing views emphasise privacy concerns regarding the handling of personal ID information by social media platforms, the lack of access to government-issued ID among many marginalised groups, and the reliance on anonymity for safety by whistleblowers and activists.

Several social media companies have introduced some form of ID verification, though the extent and implementation vary. For example, Facebook and Instagram offer ID verification for specific purposes, such as account recovery or participation in the Meta Verified programme, which provides a blue checkmark for verified users. X has introduced ID verification through its blue tick subscription service, where verified users receive a blue checkmark, and Snapchat verifies the identities of high-profile users and entities, often referred to as Snap Stars. These platforms primarily focus on verifying influential users or those who opt into specific programmes, rather than requiring ID verification for all users. In some cases, the verification services are offered as paid-for features.

Taking a broader perspective, the ID verification industry is experiencing significant global expansion, driven by increasing demand for secure online transactions and regulatory compliance. Jumio, Onfido and Liquid are examples of ID verification providers offering advanced solutions for document verification, facial recognition and data matching. According to a 2024 report[15] by MarketsandMarkets, the global ID verification market was valued at $10.9 billion in 2023, with a forecast value of $21.8 billion by 2028. As international regulations become more stringent, demand for these services continues to rise, positioning ID verification as a significant sector in the digital landscape.

Payment service providers

PSPs and banks are addressing scams using a combination of technology, collaboration and customer-focused strategies to adapt to a landscape with increasing digital transactions and associated risks, such as fraud.

[15] Identity Verification Market, MarketsandMarkets, 2024

From a technology perspective, PSPs and banks are employing advanced AI and machine-learning tools to analyse transaction patterns in real-time and identify anomalies. In Singapore, for instance, DBS Bank uses AI to monitor transactions and block suspicious ones, while Australia’s Commonwealth Bank has implemented behavioural analytics to detect if a customer's actions indicate possible coercion by a scammer. Chinese PSPs Alipay and WeChat Pay have incorporated facial recognition and device fingerprinting to prevent unauthorised access.

Additionally, more banks are starting to use GSMA Open Gateway APIs to improve their fraud prevention measures. Banks in Australia and Singapore are at the forefront of this effort, leveraging the GSMA Open Gateway's SIM Swap API to identify unauthorised SIM swaps.

Many PSPs and banks have implemented alert systems for processing transfers, in compliance with regulatory requirements. Customers receive real-time alerts about suspicious transactions via pop-ups or texts, prompting them to verify the authenticity of their transactions. In the Philippines, PSP GCash issues in-app warnings and public adverts to educate users on fake loan scams. Banks in Malaysia are incorporating additional identity checks into online banking to enhance security while maintaining convenience (as too much friction could deter some users). In Singapore, PSPs and banks have adopted the SSIR, which labels unregistered messages as “Likely-SCAM”. AsiaPay, operating across 12 countries, integrates fraud detection into its payment platforms, monitoring for indicators such as unusual IP addresses or rapid transactions.

Industry-led collaboration

In addition to government-led collaborative mechanisms, private sector stakeholders are collaborating to share intelligence on scam trends and develop solutions to protect their customers. These partnerships enable industry players to complement each other's efforts in addressing the scam economy. For instance, telecoms operators provide the infrastructure to block scam communications at the network level, while digital platform providers address the digital spread of fraudulent activities. Banks and PSPs monitor financial transactions and detect unusual behaviour and account takeovers, enhancing customer protection by integrating this information with real-time call and SMS data from operators to identify and prevent potential scams.

In Asia Pacific, where mobile penetration and social media usage are among the highest globally, collaboration is essential. For example, scam hubs in Southeast Asia frequently use telecoms spoofing and social media baiting, making these cooperative efforts crucial. Despite challenges, including cross-border coordination and adapting to AI-driven scam techniques such as deepfakes, private sector stakeholders in Asia Pacific are increasingly adopting proactive, cross-industry strategies to address the region's scam economy, as illustrated in Table 3.

Table 3: Examples of industry collaboration to tackle the scam economy

Source: GSMA Intelligence

Stakeholders	Description
Telstra, CommBank	In February 2025, Telstra and CommBank developed fraud detection technology to securely share data on unusual mobile service usage, aiming to protect consumers from identity theft. This fraud indicator service is projected to enhance the detection rate for fraudulently opened accounts by more than 25% for customers of both CommBank and Telstra.
Airtel, Boom, Dream Sports, Fortinet, Google, Meta, Microsoft, Newschecker, Shiprocket, Truecaller, Vodafone Idea and Zupee	In February 2025, digital service providers in India launched the Safer Internet India coalition. This aims to address challenges such as fraud and scams while promoting responsible innovation and digital adoption. The coalition seeks to unite nearly 1 billion digital citizens and various public and private institutions to enhance trust, safety and innovation in India's digital economy.
Globe Telecom, Meta	Globe Telecom has partnered with Meta to address text and online scams that often originate from – or are amplified through – social media. In 2023, Globe reported blocking more than 1.1 billion scam messages in the first quarter, partly by collaborating with Meta to identify and remove fraudulent accounts linked to SMS scams. This partnership supports the Philippines' SIM Registration Act, improving traceability of scam-related numbers promoted on Meta's platforms. They also conduct joint awareness campaigns, such as Globe's #SafeWithGCash initiative, extended to Meta's user base, educating Filipinos on phishing and fake promotions.
Singtel, TikTok	In 2024, Singtel entered into a partnership with TikTok to enhance anti-scam efforts under Singapore's SRF. Singtel employs network-level call and SMS filtering to identify scam communications, while TikTok uses AI to detect and remove scam content on its platform. Together, they have focused on combating 'pig butchering' scams, where fraudsters establish trust through TikTok videos before transitioning victims to SMS or phone calls.
Telstra, X	Telstra has collaborated with X to tackle scams across phone networks and social media, focusing on Australian and Asia Pacific users. In 2024, Telstra's Scam Shield blocked more than 15 million scam calls, while X improved its Community Notes feature to identify scam posts often associated with spoofed Telstra numbers. The partnership involves real-time data sharing, allowing Telstra to trace scam numbers advertised on X and enabling X to suspend accounts more quickly. This initiative is part of Australia's Scam-Safe Accord, focusing on cross-border scams originating from Southeast Asia.
PLDT, Meta	PLDT collaborates with Meta to fight scams using SMS and social media. In 2023, PLDT's Cyber Security Operations Group blocked 2.5 million scam texts monthly, often linked to Facebook Marketplace fraud or impersonation scams. They share scam number databases, enabling Facebook to shut down pages and groups promoting these numbers. This partnership has significantly reduced text-to-social scams that direct users to join fraudulent Facebook schemes, supporting PLDT's anti-fraud efforts in Southeast Asia.

4. The open API opportunity

The GSMA Open Gateway initiative, launched in February 2023, aims to harness the capabilities of mobile networks worldwide by providing access through standardised APIs. There are now 21 APIs in operation, 10 of which address anti-fraud use cases. As of February 2025, 72 operator groups, representing 284 networks and covering 78.5% of mobile connections, had committed to the initiative.

The anti-fraud response

Security protection and fraud mitigation are key applications of GSMA Open Gateway APIs used by operators and their partners. This field includes APIs such as SIM Swap, One-Time Password (OTP) and KYC Match. Additionally, Scam Signal, a joint initiative by GSMA and UK Finance, was launched commercially in November 2024 to address authorised push payment fraud in the UK. Scam Signal is designed to improve fraud detection by allowing collaboration between operators and banks, strengthening defences against scams that often impersonate trusted entities such as banks. A pilot programme showed that this initiative enhanced scam detection by 30% at one of the UK's major banks.[16]

The GSMA Open Gateway equips operators with advanced analytics tools to identify suspicious patterns, enhance security measures, detect fraudulent activities in real time, and prevent scams before they impact consumers. The anti-fraud APIs – Number Verification, SIM Swap and OTP – enable several crucial functions. Number Verification allows operators to confirm a user’s mobile number without the need for bulky SMS codes, reducing risks from intercepted messages. SIM Swap identifies recent SIM changes linked to a number – essential to preventing account takeovers. OTP provides secure, single-use codes via SMS, enhancing authentication for high-value transactions.

The initiative also fosters a unified ecosystem involving global operators and standardised APIs through the CAMARA project – an open-source collaboration with the Linux Foundation. This ensures developers worldwide can access consistent fraud-prevention tools across networks, without the need to develop separate solutions for each operator. Operators can take advantage of this to develop scalable solutions to address scams and other fraudulent activities. Furthermore, Open Gateway accelerates response times by exposing network capabilities, such as real-time device location or SIM status, to developers and financial institutions. This allows operators to flag suspicious activity instantly. The tools assist banks in verifying if a phone number's SIM was recently swapped before approving a transaction, effectively thwarting scammers.

GSMA Open Gateway also facilitates data sharing between telecoms operators and financial institutions. For instance, the authorised push payment scam prevention use case assists banks in detecting and preventing bank transfer scams by analysing network traffic data. Consequently, GSMA Open Gateway transforms telecoms networks into active shields rather than mere

[16] "GSMA and UK Finance Launch Scam Signal to Combat APP Fraud in the UK". The Financial Analyst, November 2024

pipelines, enabling operators to share intelligence and collaboratively block threats. Moreover, its scalable and collaborative foundation allows operators to proactively respond to emerging types of threat.

The GSMA Open Gateway initiative has been introduced by operators across several markets in Asia Pacific. Notably, Indonesia and Sri Lanka have launched the highest number of APIs so far. In Sri Lanka, all four major mobile operators have deployed three essential APIs: OTP Validation, Device Location and Carrier Billing. Similarly, in Indonesia, the leading operators have introduced three critical APIs: Number Verify, SIM Swap and Device Location. Australian operators are employing the Scam Signal API to identify and block scam calls and messages in real-time, while operators in the Philippines have implemented the Scam Signal API and SIM Swap API to collaborate with financial institutions on fraud detection and prevention.

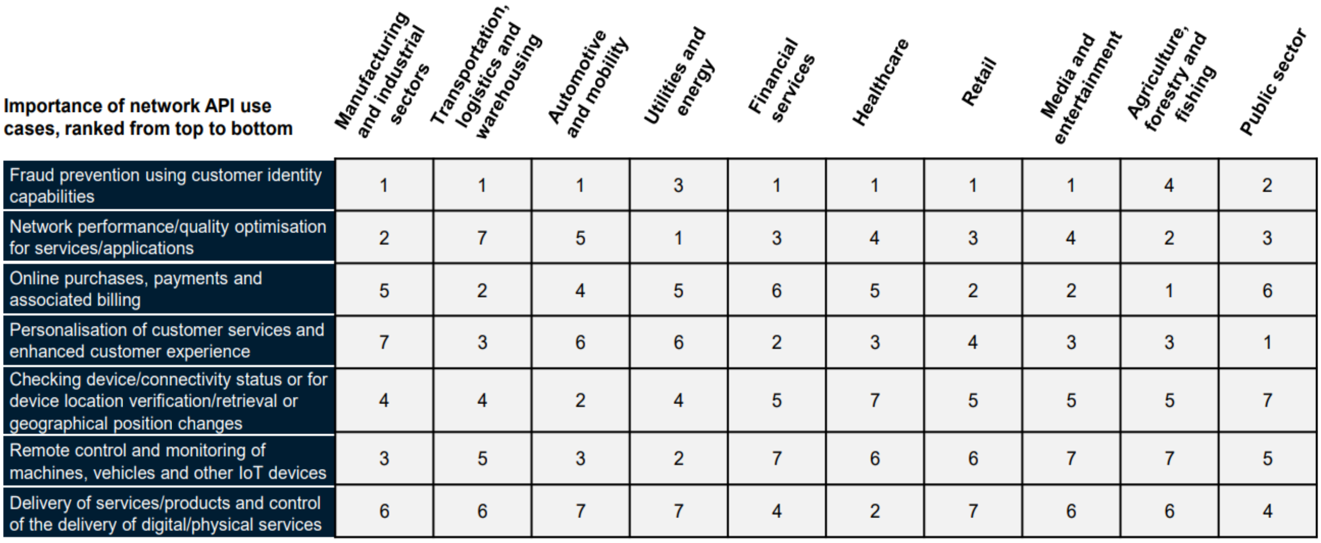
The potential for monetisation

Operators have traditionally positioned their anti-scam initiatives as measures to reduce financial losses and protect their reputations. This remains important due to the significant costs and negative impacts associated with scams. However, combating scams can be an opportunity to drive revenue growth, improve customer loyalty and benefit from the expansion of the digital economy. Some operators are already adopting this proactive approach, recognising the potential for growth in addressing scam-related issues.

The GSMA Open Gateway offers operators an opportunity to monetise their efforts in combating the scam economy by providing customised anti-fraud solutions to enterprises. According to a GSMA Intelligence enterprise survey in 2024, fraud prevention was the most attractive use case for network APIs across various sectors (see Figure 4).

Figure 4: Network API use cases ranked by importance

How important are the following network API-enabled purposes to your company's digital transformation?
Source: GSMA Intelligence Enterprise in Focus: Global Digital Transformation Survey 2024



Importance of network API use cases, ranked from top to bottom	Manufacturing and industrial sectors	Transportation, logistics and warehousing	Automotive and mobility	Utilities and energy	Financial services	Healthcare	Retail	Media and entertainment	Agriculture, forestry and fishing	Public sector
Fraud prevention using customer identity capabilities	1	1	1	3	1	1	1	1	4	2
Network performance/quality optimisation for services/applications	2	7	5	1	3	4	3	4	2	3
Online purchases, payments and associated billing	5	2	4	5	6	5	2	2	1	6
Personalisation of customer services and enhanced customer experience	7	3	6	6	2	3	4	3	3	1
Checking device/connectivity status or for device location verification/retrieval or geographical position changes	4	4	2	4	5	7	5	5	5	7
Remote control and monitoring of machines, vehicles and other IoT devices	3	5	3	2	7	6	6	7	7	5
Delivery of services/products and control of the delivery of digital/physical services	6	6	7	7	4	2	7	6	6	4

By customising the APIs for different industries, the GSMA Open Gateway initiative unlocks new opportunities and enhances capabilities across various sectors. Examples include the following:

- **Finance –** The SIM Swap and Number Verification APIs assist banks and financial institutions in identifying and preventing identity theft and fraud. They help ensure the security of transactions and the accurate verification of customer identities.

- **Healthcare –** The Device Location and Quality on Demand (QoD) APIs can be utilised in telemedicine to guarantee high-quality video consultations and precise location tracking for emergency services.

- **Retail and e-commerce –** The Carrier Billing API enables the smooth integration of payment services, allowing customers to make purchases directly through their mobile operator. This streamlines the checkout process and enhances customer experience.

- **Entertainment –** The Edge Site Selection API optimises the delivery of high-definition video and immersive gaming experiences, ensuring low latency and high-quality streaming for users.

- **Transport and logistics –** The Device Status and Verify Location APIs aid in tracking shipments and managing fleet operations more efficiently. They provide real-time updates on the status and location of vehicles and goods.

In addition to providing fraud prevention services through the GSMA Open Gateway APIs, operators have opportunities to serve enterprises with anti-fraud solutions. For example, operators can offer specialised fraud prevention services, such as real-time transaction monitoring and risk assessment. Another opportunity lies in developing and selling advanced data analytics and AI-powered fraud detection solutions that can analyse extensive data to identify suspicious patterns and prevent fraudulent activities. This can deliver significant value to enterprises across multiple sectors. Forming partnerships with financial institutions and other stakeholders is crucial for creating monetisation opportunities and developing innovative fraud prevention solutions. By leveraging expertise in fraud prevention, operators can develop valuable products and services that drive revenue and contribute to a safer digital environment.

Telkomsel: improving digital authentication through network APIs

Background

Amid growing cybersecurity risks, smartphones are increasingly expected to replace traditional authentication methods such as passwords This is being driven by the enhanced convenience and security features that smartphones offer, as well as new digital authentication solutions.

Challenge

As the security threat landscape evolves, growing levels of consumer engagement with digital services – particularly via smartphones – present greater exposure to identity fraud. Banking and financial transactions are particularly at risk. In Indonesia, digital banking transactions reached nearly $4 billion in 2023. In parallel, there were around 360 million cyberattacks, of which 42% were malware-based, 35% via trojans and 9% using information leaks. There is a clear risk of financial loss for consumers, businesses and financial institutions.

Solution

Telkomsel has developed an identity solution called Telco Verify. This works via a network API and is designed to add an additional layer of security to the authentication process. The solution can be added to existing mechanisms such as two-factor-authentication (2FA) and one-time passwords. The incremental value is the explicit link of a mobile number to a person. If a person has a new mobile, for example, Telco Verify can be used to authenticate that individual when registering their mobile banking account on the new device.

Impact

Telco Verify looks to blunt the risk of identity fraud through websites, digital banking and other interfaces requiring personal credentials – anything from a government login to the purchase of a concert ticket. Indonesia has a high-growth economy and a youthful, digital-native population. Digital banking values reached IDR58 trillion ($3.7 billion) in 2023. The country has also introduced a QR-based payment system (QRIS) now used by around 15% of the population. Given that most digital payments are via mobile, Telco Verify can help materially reduce the risk of fraud.

5. Future outlook and considerations

Protecting consumers and preserving trust in the digital world will remain a priority for governments, operators and stakeholders in the digital ecosystem. This is essential to sustain the growth of digital services and their contribution to socioeconomic progress, aligning with the digital ambitions of governments across Asia Pacific. Addressing the scam economy is crucial to achieving this goal, given the erosive effect that online scams and fraudulent activities can have on user trust. Stakeholders have already taken steps in this direction. However, with the constantly evolving online threat landscape, there are key considerations for stakeholders going forward.

Post-fraud support for victims

While efforts by stakeholders to address scams are proving effective, there remain instances where individuals fall victim due to a range of factors, which may include data breaches at organisations holding their personal information. Victims experience emotional, financial and practical repercussions that can exacerbate without appropriate assistance.

Prompt support can mitigate long-term harm and potentially disrupt scammers' operations by empowering victims to take action. A 2023 AARP study revealed that 80% of scam victims reported experiencing anxiety, shame or depression, with some encountering PTSD-like symptoms. Support services such as counselling or peer groups (e.g. Australia’s ScamSafe network) play a crucial role in helping individuals process the betrayal and regain confidence. In the absence of such support, isolation can intensify, leading some individuals to withdraw from digital life entirely, which is not a viable solution in today's interconnected world.

Many victims lose significant amounts of money to scams, potentially leaving them without a livelihood. Post-fraud assistance, such as the UK's Action Fraud reimbursement programmes or Singapore's bank-led recovery schemes, can recover funds, sometimes through frozen accounts if reported promptly.

The availability of legal aid can also provide support by guiding victims through disputes or small claims against fraudsters or negligent platforms. Post-fraud support is also crucial in preventing further losses. Data from the US FTC indicates that one in five victims are re-targeted within a year, often using stolen personal information.[17] Recovery services, such as identity theft protection or telecoms call-blocking upgrades, help mitigate these risks. Education is also essential, as teaching victims how to identify red flags can reduce repeat losses.

Assisting victims in reporting fraud enhances enforcement efforts. In 2024, Japan saw a significant increase in tip-offs to police through post-fraud hotlines, which led to a higher number of arrests.[18]

[17] See www.ftc.gov/news-events/data-visualizations

[18] "Record loss from fraud and social media scams reported in 2024", The Asahi Shimbun, February 2025

This surge in reports and subsequent police action have been crucial in tackling fraud, including special fraud cases and scams involving social media and investment fraud. Collecting recovery data also improves prevention measures. For example, banks and regulators can use this information to identify scam patterns. Without support, victims tend to deteriorate further, with some resorting to borrowing in an attempt to recover. Others fall victim to fraudulent recovery scams that promise to return lost funds. The repercussions extend to families and communities too, eroding trust and resources.

The role of AI and other emerging technologies in addressing scams

Emerging technologies can help combat scams from multiple angles. The technologies can detect fraudulent activities more quickly, prevent unauthorised access and expose deceptive schemes. Notably, AI plays a pivotal role in both facilitating and preventing scams. When utilised by malicious individuals, it can be a tool for conducting fraudulent activities and complicating efforts to prevent such actions. However, AI also holds the potential to enhance anti-fraud measures when properly applied.

AI is currently being integrated into various anti-scam solutions, though there remains considerable opportunity to develop new applications to continually outpace scammers who are also employing the technology. One promising area involves using AI to predict scam trends before they become widespread. Another innovative prospect is AI-powered 'scam-baiting', where bots are trained to engage with scammers, wasting their time and gathering information to apprehend them. Nonetheless, stakeholders must balance these opportunities with any privacy and ethical considerations.

In addition to AI, other emerging technologies may help combat scams. Blockchain is notable for its impact on financial fraud. Its decentralised, tamper-proof ledger can make fraudulent transactions more difficult to execute. For example, blockchain can verify supply chains or identities without relying on intermediaries – though it is not foolproof, as scammers exploit it when users lack understanding. Quantum computing is another potential tool, capable of breaking encryption used by scammers, revealing their actions. However, it could also enhance scammers' ability to breach security systems, presenting both opportunities and risks.

Biometrics, including facial recognition and behavioural patterns (such as typing habits), could strengthen defences against identity theft but must be balanced with the protection of privacy and personal data. Edge computing, which processes data locally rather than in the cloud, may enhance real-time fraud detection on devices such as smartphones, potentially reducing the risk of scams by limiting reliance on central servers and shrinking the attack surface.

Augmented reality (AR) also holds promise. For instance, AR glasses could alert users to phishing links in their field of vision, providing proactive protection. While currently niche, AR technology may become more widespread as costs fall.

Each of these technologies has specific advantages, but all must navigate challenges such as cost, adoption and the evolving tactics of scammers.

The digital ‘arms race’ among ecosystem participants such as operators, digital platforms and PSPs against increasingly sophisticated scammers relies heavily on the ability of service providers to invest in and quickly deploy new, innovative solutions. This requires not only a significant financial commitment but also the fostering of a culture centred on continuous development and adaptation.

The complexity of this challenge is further compounded by varying levels of market maturity. Technologically advanced markets can adopt cutting-edge anti-fraud measures with relative ease, whereas emerging markets often face infrastructure constraints and regulatory deficiencies, leading to a fragmented landscape prone to exploitation by scammers. This disparity highlights the critical need for robust cross-border collaboration, necessitating that providers, regulators and technology developers work together to share threat intelligence, standardise best practices and develop interoperable solutions to effectively combat scams across diverse market environments.

Opportunities to monetise anti-scam solutions

For industry stakeholders, combating fraud serves to protect businesses and consumers while also presenting monetisation opportunities. The previous section discussed the potential for operators to use anti-fraud APIs as part of the GSMA Open Gateway initiative to assist enterprises across sectors. Beyond enterprise solutions, the growing need to protect consumers from scams could present monetisation opportunities.

For operators and other industry participants, customer loyalty is a significant economic benefit of fighting scams. Protecting customers helps brands retain them, which often leads to higher retention rates and provides cross-sell opportunities. This can act as an incentive to address scams and potentially recover some of the investments in anti-scam solutions.

In addition to fostering customer loyalty, operators can generate direct revenue by investing in innovative technologies and offering premium anti-scam solutions as optional value-added services. These solutions could include advanced authentication methods such as biometric verification through APIs, the option to upgrade to enterprise-grade security features tailored to high-risk accounts, and proprietary applications that filter spam calls, block phishing attempts and provide real-time scam detection. Furthermore, service plans can offer additional data privacy protections, such as enhanced encryption, anonymisation and reduced data sharing.

Some operators provide basic scam protection tools at no cost, with advanced opt-in solutions available for a fee. For instance, T-Mobile US offers free scam protection tools such as Scam ID and Scam Block to all contract customers. These identify and block suspected scam calls. It also offers a premium service called Scam Shield Premium for an additional fee (approximately $5 per month as part of its Protection 360 plan or standalone in some cases). This includes enhanced features such as voicemail-to-text, advanced call blocking for categories such as telemarketers, and a reverse number lookup tool. The premium tier builds on the free baseline protections, catering to users seeking more control.

Similarly, Verizon offers a basic Call Filter service for free, which flags suspected spam calls. Call Filter Plus comes with a premium charge, typically $2.99 per month, per line or $7.99/month for up to 10 lines. This upgraded version includes caller name identification, a personal block list and a spam risk meter, appealing to customers seeking deeper protection against scams.

Digital platform providers have also developed monetisation strategies as part of efforts to address scams, which can inconvenience users and deter advertisers. By implementing ad verification measures to eliminate fraudulent advertisements, the platforms are able to charge legitimate advertisers a premium for ‘trusted placement’ badges or analytics that demonstrate their ads are reaching actual users rather than bots. X is evolving its verified status into a tiered subscription model, offering scam-proof benefits such as priority support and enhanced privacy for higher fees. Similarly, Meta allows businesses on its marketplace to pay for a verified badge.

Another potential opportunity lies in data monetisation. Both operators and social media providers have vast repositories of behavioural data, including call patterns, app usage and browsing habits. Their ability to anonymise, mask and analyse this data in real time for scam prevention can also be leveraged for revenue-generating services. For instance, anonymised threat insights could be marketed to banks or insurers, who might be willing to invest in such information to strengthen their own security measures. Although this opportunity may be limited in scenarios where certain data-sharing mechanisms are in place, the insights derived from advanced analysis could still command a premium.

Ecosystem-wide collaboration to combat scams

The pervasive nature of the scam economy requires collaboration from all players, including mobile operators, digital platforms and PSPs. These possess complementary strengths essential for effective scam prevention. Operators have extensive network data, including call patterns, location information and device identifiers, offering a unique perspective for detecting unusual activity. Digital platforms and PSPs, meanwhile, have detailed user behavioural data and content analysis capabilities to identify fraudulent patterns within systems. By integrating these datasets, a combined data advantage is achieved, providing a more comprehensive and real-time view of potential scams. The integration also enhances real-time detection by allowing real-time analytics and AI algorithms to be shared and combined for quicker identification and mitigation of emerging scam threats.

Collaboration transcends mere data sharing to encompass the development of interoperable solutions and standardised protocols. This facilitates seamless information exchange and coordinated responses across platforms and networks, fulfilling the need for standardised protocols and interoperability. Cross-platform threat intelligence is essential. Shared threat intelligence, including known scam tactics, fraudulent numbers and malicious URLs, enables proactive blocking and mitigation measures.

A key advantage of collaboration lies in the benefit of having multiple points of verification and authentication across media and platforms. For instance, as part of TikTok's business account registration process, the assessment team evaluates whether the applicant has verified IDs from other notable platforms. This cross-referencing of verified data enhances the overall authentication process, adding layers of trust and significantly impeding scammers' operations.

A unified approach is also crucial as scammers continuously adapt and migrate to different platforms when detection mechanisms become stricter. Without coordinated efforts, fraudsters can exploit gaps between ecosystems, rendering isolated security measures less effective. By fostering collaboration, businesses and regulators can establish a more robust and resilient digital environment, where threats are addressed proactively rather than reactively, reducing the overall impact of scams.

The fight against scams is ultimately a collaborative effort. Consumers expect a secure digital experience, and the reputations of mobile operators and digital platforms depend on their ability to provide it. By adopting a collaborative approach, they can use their combined resources and expertise to stay ahead of evolving threats. This partnership is not merely a defensive measure but also an opportunity to build trust, enhance customer loyalty and demonstrate a commitment to protecting the digital ecosystem.

Secure digital transformation initiatives

As countries work towards their digital nation goals, emerging technologies such as IoT, AI, cloud computing and virtualisation will play a crucial role in creating smart solutions across sectors, including healthcare, urban planning, utilities and transport. This expansion may introduce new areas of potential vulnerabilities for unauthorised access to the personal data of individuals and businesses using these services where security is insufficient. For instance, IoT devices, such as smart home systems and wearables, could be targeted due to inadequate security measures. These vulnerabilities can be exploited to gain access to networks and sensitive information.

A secure digital environment enhances innovation by reducing the risks associated with emerging technologies and services. This supports the advancement of sophisticated solutions in areas such as IoT, smart cities and fintech, generating new market opportunities. It is therefore crucial for stakeholders to safeguard the digital environment to foster innovation and ensure the continuous and reliable operation of smart systems within a digital nation. This involves protecting connected devices and other digital assets, given the significant impact breaches can have on public trust.

A collaborative approach to addressing cross-border scams

International collaboration is crucial in addressing scams, since fraud transcends borders, enabling perpetrators to operate across jurisdictions effortlessly. Many scams, such as phishing, romance scams or investment cons, are digital in nature, often orchestrated from one country, targeting victims in another and laundering profits through a third jurisdiction.

The primary challenges in tackling cross-border scams include: logistical issues, where scammers use technology such as VPNs, offshore servers and encrypted applications to obscure their activities; discrepancies in legal frameworks, which create potential loopholes for exploitation; the rapid pace and high volume of attacks, which can overwhelm individual regulators; and the extensive reach of global operators and social media platforms, necessitating coordinated efforts to ensure an effective response.

Countries in Asia Pacific are increasingly collaborating internationally to combat scams, recognising that cyber fraud is a transnational issue requiring coordinated action. Their efforts include intelligence sharing, joint operations, policy alignment and capacity building, often facilitated by regional and global organisations.

For instance, ASEAN has committed to tackling online scams, with a focus on cross-border law enforcement. An example is Thailand and Cambodia's joint operation in mid-2024, where police collaborated to raid scam centres exploiting trafficked workers for fraud schemes such as ‘pig-butchering’ romance and investment scams originating from Southeast Asia.

The Asia-Pacific Economic Cooperation forum supports trade-focused initiatives, such as Australia funding capacity-building in Papua New Guinea and Vietnam to improve digital literacy and regulatory frameworks against scams. Such efforts complement broader initiatives such as ASEAN’s Digital Economy Framework Agreement, which promotes secure cross-border technology standards.

Additionally, the Global Anti-Scam Alliance and the Tech Against Scams Coalition facilitate real-time scam data sharing among Asia Pacific nations such as Singapore and Japan, along with technology firms such as Meta and Coinbase. Singapore's 24×7 anti-scam hotline and Malaysia's National Scam Response Centre also contribute to these regional and global networks.

Privacy and ethical considerations

With the rise of more sophisticated scams and other online attacks, governments and policymakers, operators and other digital ecosystem players naturally want to act to prevent such incidents and protect citizens to the greatest extent they can, using anti-scam solutions. In this context, privacy and ethical considerations in anti-scam solutions are crucial to ensure the protection of individuals' data and to maintain trust. These help create a balanced approach that protects users while effectively combating scams. The GSMA reports AI Ethics Playbook and Safety, privacy and security across the mobile ecosystem outline key privacy and ethical considerations for digital ecosystem stakeholders in the development of solutions to tackle the scam economy.

Call to action: Realising the potential of ecosystem-wide collaboration

Articulate the positive outcomes of collaborative actions to address the scam economy

To enhance the understanding of collaborative anti-scam efforts, it is important to present success stories and share best practices. This involves documenting and sharing instances where joint initiatives have successfully prevented scams, emphasising the benefits of cross-ecosystem collaboration.

By developing case studies, publishing reports and organising community forums, the industry can encourage wider adoption of effective strategies. This narrative will demonstrate the effectiveness of collaborative approaches and provide a resource for industry stakeholders, promoting continuous learning and collectively advancing fraud prevention measures. Most importantly, these efforts will help victims be better supported and protected, reinforcing their trust in the system.

Establish a unified ecosystem to enhance progress and counter new threats

To effectively address the scam economy, operators and digital platform players need to move beyond traditional silos and engage in ecosystem-wide collaboration. This involves the timely sharing of threat intelligence, the joint development of standardised frameworks and protocols, and the integration of complementary data sources. Forming cross-functional working groups and a community are crucial to promote collaborative innovation and knowledge sharing.

By combining diverse expertise and perspectives, these groups can further the development of anti-fraud solutions and establish a continuous feedback loop for quick adaptation. Adopting a collaborative framework will help create a dynamic, adaptive defence that mitigates current threats and anticipates emerging fraud tactics, ensuring a safer digital environment for all. This unified approach will prioritise the needs of potential victims, providing them with the necessary protections and support to feel more secure in the digital world.

Further reading

The Mobile Economy 2025

Fraud and Scams: Staying Safe in the Mobile World

Telco security landscape and strategies: Asia Pacific

Consumer Attitudes Toward Fraud and Opportunities for Mobile Network Operators in SEA

The GSMA Responsible AI Maturity Roadmap

GSMA Intelligence

gsmaintelligence.com