GSMA Intelligence

Towards an inclusive digital nation: addressing the scam economy and preserving trust in the digital ecosystem

March 2025

GSMA

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

Follow the GSMA on X: @GSMA

GSMA Intelligence

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, APAC
Syed Khairulazrin Bin Syed Khairuldin, Policy Director, APAC
Ming Sheng Bensen Koh, Senior Policy Manager, Southeast Asia

Contents

Executive summary

The rapid expansion of digital technologies, particularly mobile connectivity, has profoundly impacted both the techniques and the reach of scams. Today, essentially every individual with a mobile subscription – approximately 5.8 billion people, including 4.7 billion who also use mobile internet – is a potential target for contemporary scams. The constant rise in the volume, frequency, sophistication, and success rate of scams in recent years is 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 over $1.03 trillion worldwide over the past year.[i] This increasing incidence of scams and their associated financial consequences is commonly referred to as the "scam economy."

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

Preserving trust in the digital world will undoubtedly remain a top priority for governments, operators, and stakeholders within the digital ecosystem. This is essential to sustain the growth of digital services and their contribution to socio-economic progress, aligning with the digital ambitions of governments across the Asia-Pacific region. 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 continue build on existing 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; collaborative approach to addressing cross-border scams; post-fraud support for victims; and privacy and ethics considerations.

Looking ahead, 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 by actively documenting and sharing instances where joint initiatives have successfully prevented scams, and by highlighting the tangible benefits of cross-ecosystem collaboration. Furthermore, 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.

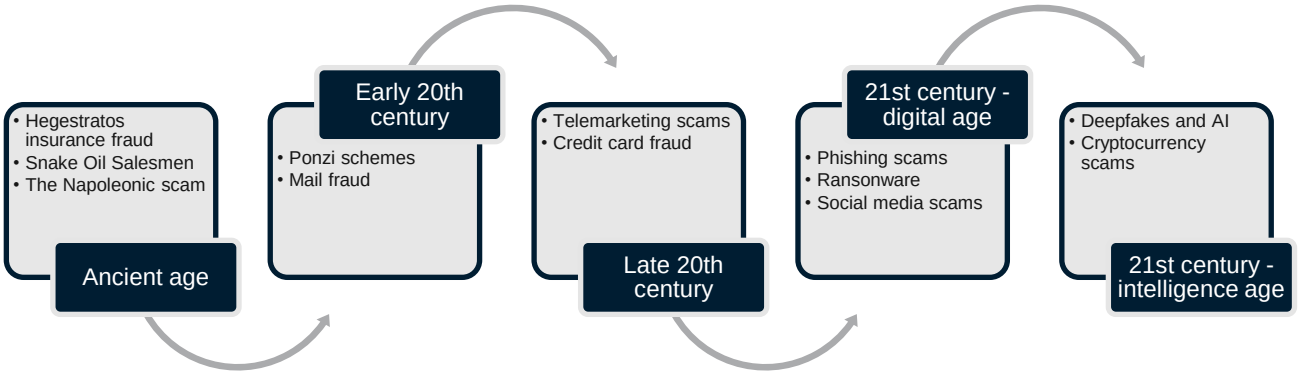
1. Introduction: the scam economy

Scams have been a part of human interaction throughout history, as documented in various records. From ancient mythologies, such as the story of the Trojan Horse, to real historical events, there are numerous examples of activities that align with today's definition of a scam. The Cambridge Dictionary defines a scam as "_a dishonest plan for making money or gaining an advantage, particularly one that involves deceiving people_". While the underlying principles and motivations behind scams have remained consistent across generations and cultures, the methods have evolved and adapted in response to societal changes over time.

Since the 20th century, technological advancements have significantly influenced the evolution of scam methods. This progression has transitioned from simple, physical tactics, such as sinking cargo ships for insurance claims, to sophisticated scams employing digital technologies (Figure 1). Over the past three decades, the rapid expansion of digital technologies, particularly mobile connectivity, has profoundly impacted both the techniques and the reach of scams. Today, essentially every individual with a mobile subscription – approximately 5.8 billion people, including 4.7 billion who also use mobile internet – is a potential target for contemporary 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 through other means, such as via a friend or relative.

Figure 1: Examples of scam methods over time

Source: GSMA Intelligence



Today, scams are more prevalent online compared to offline due to various factors that make the digital environment attractive to scammers. Some of these factors are highlighted below:

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 compared to 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 email 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 many daily transactions, certain practices, such as social media oversharing and inadequate security resulting in data breaches, 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. In contrast, offline scams are typically confined to a single jurisdiction, which allows authorities to more easily track perpetrators.

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

Technological 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 these innovations, creating opportunities for exploitation by scammers.

The scope of online scams is extensive and varied, with scammers employing numerous tactics. Examples include: phishing (emails that imitate those from credible organisations); smishing (SMS messages that seem to be from reputable companies); vishing (phone calls that impersonate legitimate entities); spoofing (false caller ID information so the call appears to be from a trusted source); digital arrests (impersonation of law enforcement via video calls); romance scams (emotional manipulation); and pop-up notifications (fake alerts prompting users to click on a link or call a number). In the Asia Pacific region, the “pig butchering” scam (a long-term fraud involving tricking victims into investing in a fake cryptocurrency scheme) has become prevalent, particularly in countries like Myanmar, Cambodia, and Laos, where these operations also involve human trafficking.[ii]

While these and other tactics have existed since the advent of the digital age, they have been significantly enhanced by Artificial Intelligence (AI). This enhancement is evidenced by the marked increase in scam activities in recent years. 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), and automated social engineering (using AI to analyse social media profiles and other online data to craft convincing messages that exploit personal details). From 2022 to 2023, Asia Pacific experienced a 1,530% increase in deepfake fraud. Countries like Malaysia, Singapore, and Indonesia have issued warnings about these high-tech scams, which use manipulated videos and audio to deceive victims.[iii]

The constant rise in the volume, sophistication, frequency, and success rate of scams in recent years is 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 over $1.03 trillion worldwide over the past year.[iv] The report highlights that individuals in the United States experienced the highest losses, with an average of $3,520 per victim.

Countries in the Asia Pacific region are also facing substantial economic costs due to fraudulent activities. For example, in India, over INR11,000 crore (approximately $1.5 billion) was lost to online scams during the first nine months of 2024, with stock trading and investment scams being the most frequently reported cases. [v] In Thailand, the Anti-Online Scam Operation Centre (AOC 1441) recorded five significant scam cases within a single week in January 2025, resulting in a total loss of THB21 million (equivalent to $610,000). [vi]

The increasing incidence of scams and their associated financial consequences is 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 – including the perpetrators, the tools they use, the victims they target, and the funds extracted from them. It is important to note that the term "scam economy," which focuses more on the deception and exploitation of individuals, is a subset of a broader term, "fraud economy." The latter includes all types of fraudulent activities, affecting both businesses and institutions. Although these terms are sometimes used interchangeably, this paper will concentrate on the impact on individuals.

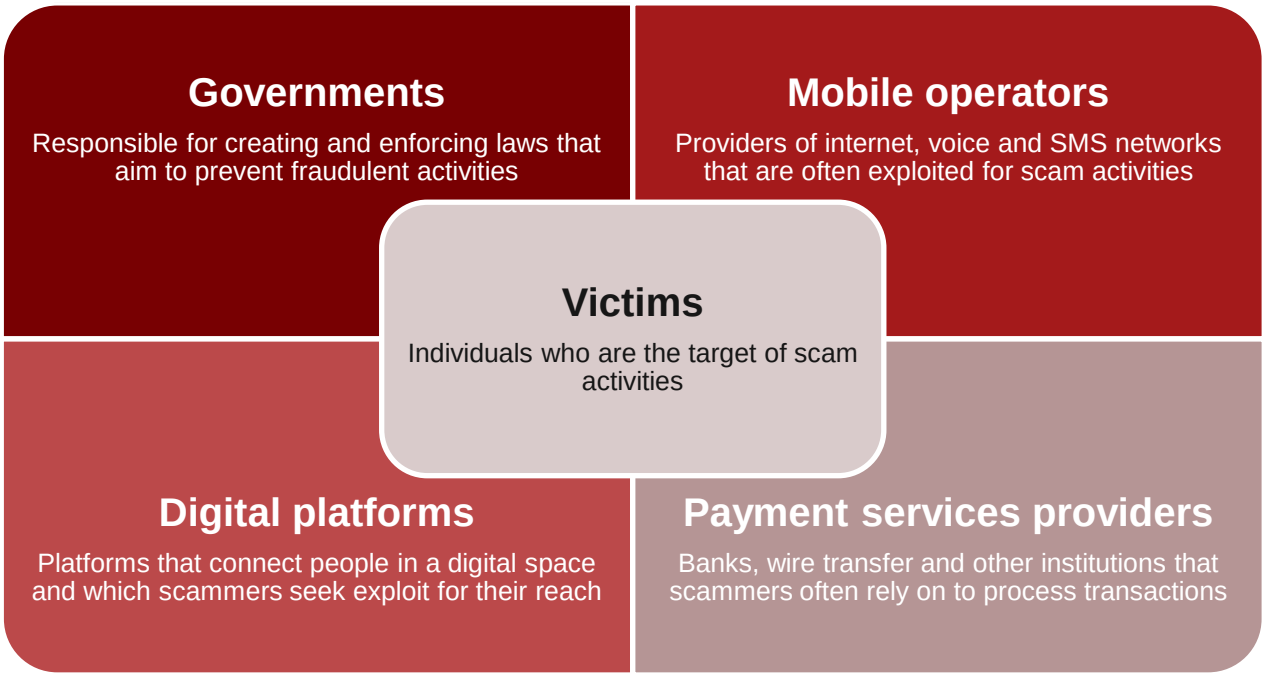
2. The impact of the scam economy

The scam economy involves various "unwilling stakeholders" in its operations. These are individuals and entities that are indirectly affected by fraudulent activities, often without their knowledge or consent, and are vulnerable to the negative impacts of these activities. A major impact of scams, which affects the entire 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. This 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) that are often entangled, and how they are impacted by these activities.

Figure 2: Individuals and entities entangled in the scam economy

Source: GSMA Intelligence



Victims

Every scam unfortunately involves a victim. These victims are often individuals who lose personal information and financial assets to scammers but can also include entities that are 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 and often include 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 also 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.

However, 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 the Asia-Pacific region and beyond. [vii]

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 governmental 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. [viii] In the Philippines, the Bureau of Immigration (BI) warned the public about scammers running fake websites charging for e-Travel registration. Similarly, New Zealand's Inland Revenue Department (IRD) in 2024 highlighted a convincing email scam targeting those awaiting tax refunds to steal personal details.

Mobile operators

Mobile operators often find their services, such as voice calls, SMS, and internet connectivity, exploited by scammers to reach victims through activities like 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. [ix] 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 actions, such as fines.

Operators must balance security and privacy considerations and are legally required to protect 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 invest significant resources in scam prevention, detection and mitigation solutions. These include 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 KYC (Know Your Customer) and OTP (One-Time Password) scams, where fraudsters deceive users into disclosing their credentials through calls or SMS. In Indonesia, operators have made substantial investments in fraud management systems, potentially diverting 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:

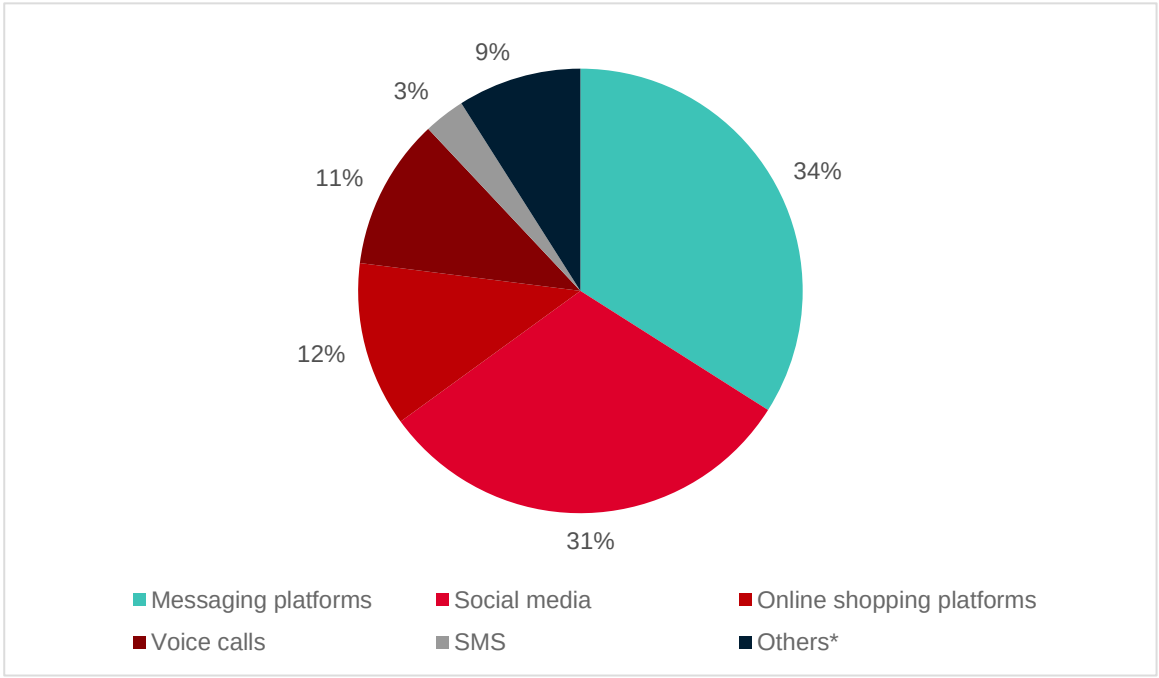
- **Social Media Platforms** – websites and apps that allow users to create, share, and interact with content, such as Facebook, X (formerly Twitter), and Instagram;
- **E-commerce Platforms** - online marketplaces where users can buy and sell products, such as Amazon, eBay, and Alibaba;
- **Content 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; and
- **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 that allows 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. The 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 indicate 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, respectively (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 their platforms less appealing to scammers. Although it can be a complex task, it is necessary for maintaining trust and safety on digital platforms.

Figure 3. Singapore: breakdown of reported scam cases based on contact methods
Source: Singapore Police Force



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. For example, companies such as Google and Meta have reported substantial investments in AI systems to address scams and other fraudulent activities.

Payment system 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 utilise PSP services to carry out 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 over $10 billion in fraud losses, much of it occurring through legitimate financial channels.[x] PSPs and banks face the challenge of releasing customers' funds upon request while also protecting them from potential scams.

The increasing adoption of digital payments has made it a prime target for fraudsters. For instance, mobile devices are implicated in 74% of global digital payment fraud incidents, reflecting the shift towards 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, [xi] a situation 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 up to $120 million and to pay a penalty of $55 million 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.[xii]

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 (BOT) mandated that all banks expedite refunds for victims of credit card fraud, ensuring compensation within five business days if the cardholder is found not responsible. Additionally, in December 2024, Malaysia's 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.

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. Consequently, stakeholders have shown a heightened focus 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 necessitates a shift from assigning blame for fraudulent activities to utilising collaborative mechanisms to effectively combat scams. Some recent initiatives by stakeholders to address the scam economy are noted below.

Government-led efforts

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

Whole-of-government approach (WGA): This strategy entails addressing the scam economy through a comprehensive cross-agency collaboration with industry stakeholders. The objective is to streamline efforts and enhance efficiencies in both the formulation and implementation of 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. [xiii]

Legislation: This establishes a structured and enforceable framework to safeguard citizens from fraudulent activities 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 to combat scams. The Australian Communications and Media Authority (ACMA) and other regulators will enforce industry codes for banks, telecoms, and social media. Telecoms must block scam SMS and calls, and social media firms must verify advertisers. The framework becomes 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 (BNM).

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 the 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 also 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 that stakeholders implement comprehensive security protocols to safeguard consumers from scams. For instance:

- In February 2025, the Securities and Exchange Board of India (SEBI) 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.

- Additionally, in December 2024, the Department of Telecommunications (DoT) in India announced the deactivation of over 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 (MAS) and IMDA jointly introduced a new Shared Responsibility Framework (SRF) 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 (CAD) of the Singapore Police Force (SPF) and Commercial Crime Investigation Department (CCID) of the Royal Malaysia Police (RMP) jointly dismantled a transnational scam syndicate involved in Government Official Impersonation Scams (GOIS) in Malaysia. In December

2024, Australian ACMA, and UK telecoms regulator the Office of Communications (Ofcom), agreed to improve information sharing and cooperation to combat phone scams, spam, and unsolicited calls.

Data Sharing: 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 the Asia Pacific region include:

- In 2023, Australia's 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 (AFASA), enacted in 2024, enhances data sharing between the Bangko Sentral ng Pilipinas (BSP), 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 telecom operators, to share data and intelligence on scam activities. This collaboration facilitates the prompt detection and disruption of scam operations. The ASCom aims to achieve greater synergy between the various scam-fighting units within the Singapore Police Force (SPF).

- At the 42nd Association of Southeast Asian Nations (ASEAN) Summit in May 2023, Southeast Asian leaders committed to strengthening cross-border data sharing to combat online scams and human trafficking. The ASEAN Senior Officials Meeting on Transnational Crime (SOMTC) 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 (UNODC), focusing on hubs in Myanmar, Cambodia, and Laos.

Awareness campaigns: These initiatives aim to educate individuals about 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, and education is a key strategy to combat it. For instance, in January 2025, the Cyber Security Agency of Singapore (CSA) 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 (PDRM) has initiated the "Stop Scams" campaign, which includes public

service announcements, social media campaigns, and community engagement activities designed to educate the public about various types of scams and preventive measures.

Telecoms operators

Telecom 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.

Additionally, 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. The table below provides examples from countries across Asia Pacific.

Table 2: 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. The solution analyses 250 parameters, such as a caller or sender’s usage patterns, call/SMS frequency, and call duration, in real-time. By cross-referencing this information against known spam patterns, the system identifies suspected spam calls and SMSs.
Axiata	Axiata has implemented its Helios platform across its operations in the Asia Pacific region, 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 utilises 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. This system is aligned with Japan’s national initiatives to combat telecom fraud through improved KYC processes.
SK Telecom	SK Telecom has implemented AI-powered fraud detection, which includes real-time network monitoring and voice biometrics. These systems analyse call data and user behaviour to identify anomalies, such as SIM box fraud or account takeovers. Additionally, SKT'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, utilising network-level blocking and AI analytics to identify and prevent scam calls, including those utilising 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 comprehensive cyber protection system designed to safeguard against online fraudulent activities in Thailand. This system offers protection from phishing links, scam SMS, and includes call filtering. By the end of January 2025, True Corporation reported that True CyberSafe successfully blocked over 370 million suspicious link clicks, thereby protecting its customers from potential scams.

Digital platform providers

Digital platform providers are addressing scams through a combination of technological tools, policy enforcement, and user education initiatives. Many platforms implement advanced algorithms and artificial intelligence 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, thereby 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 about 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 about common tactics like unsolicited messages from fake profiles. Below are some examples of the measures taken by digital platfrom companies:

Table 3: Examples of efforts by social media 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 over 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 (IC4) 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 SMSs 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.
Tik Tok	**Content Moderation:** TikTok employs artificial intelligence 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 scams.
X (formerly Twitter)	**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 checks and organisational badges) to decrease impersonation scams by making it more challenging for fraudsters to pose as legitimate personalities or brands. **Community Notes:** A user-driven feature that allows people to flag misleading posts, including scams like 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. Moreover, not all fraudulent activity is reported, which suggests that the scale of the issue may be greater than what is currently known.

One issue that remains debated about social media platforms is the introduction of ID verification for all users. Some arguments in favour of this measure 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 program, 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 programs, rather than requiring ID verification for all users. In some cases, these verification services are offered as paid features.

Considering the broader perspective, the ID verification industry is experiencing significant global expansion, driven by the increasing demand for secure online transactions and regulatory compliance. Prominent companies such as Jumio, Onfido, and Liquid Inc. are leading this sector, offering advanced solutions for document verification, facial recognition, and data matching. According to a 2024 report by MarketsandMarkets, the global ID verification market was valued at $10.9 billion in 2023, with an anticipated growth reaching USD 21.8 billion by 2028. As international regulations become more stringent, the demand for these services continues to rise, positioning ID verification as a significant sector within 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. 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.

Additionally, more banks are starting to use the 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. Moreover, Chinese PSPs Alipay and WeChat Pay have incorporated facial recognition and device fingerprinting to prevent unauthorised access.

Many PSPs and banks have implemented alert systems for processing transfers, often 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, the leading PSP GCash issues in-app warnings and public ads to educate users about 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-SCAM2." 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, telecom 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 behaviours and account takeovers, enhancing customer protection by integrating this information with real-time calls and SMS data from telecom operators to identify and prevent potential scams.

In the Asia-Pacific region, where mobile penetration and social media usage are among the highest globally, collaborations are essential. For example, scam hubs in Southeast Asia frequently utilise telecom 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 unique scam economy, as illustrated in the table below.

Table 4: Examples of industry collaboration to tackle the scam economy

Source: GSMA Intelligence

Stakeholders	Detail
Telstra, CommBank	In February 2025, Telstra and CommBank developed fraud detection technology to securely share data about 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 over 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, including Airtel, BOOM, Dream Sports, Fortinet, Google, Meta, Microsoft, Newschecker, Shiprocket, Truecaller, Vodafone Idea, and Zupee, launched the Safer Internet India (SII) coalition. This collaborative effort aims to address challenges such as frauds and scams while promoting responsible innovation and digital adoption. The coalition seeks to unite nearly a 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 or are amplified through social media. In 2023, Globe reported blocking over 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 about 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 utilises artificial intelligence 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 over 15 million scam calls annually, 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, emphasising 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 frauds 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 application programming interfaces (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 opportunity

Security protection and fraud mitigation are key applications of GSMA Open Gateway APIs used by operators and their partners. This field includes various APIs such as SIM Swap, 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 (APP) fraud in the UK. The Scam Signal is designed to improve fraud detection by allowing collaboration between operators and banks, strengthening defences against scams that often impersonate trusted entities like banks. A pilot program showed that this initiative enhanced scam detection by 30% at one of the UK's major banks.[xiv]

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, thereby reducing risks from intercepted messages; SIM Swap identifies recent SIM changes linked to a number, which is essential for preventing account takeovers; and 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 that 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, the 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. These tools assist banks in verifying if a phone number's SIM was recently swapped before approving a transaction, thus effectively thwarting scammers.

The Open Gateway also facilitates data sharing between telecommunications operators and financial institutions. For instance, the Authorised Push Payment (APP) Scam Prevention use case assists banks in detecting and preventing bank transfer scams by analysing network traffic data. Consequently, Open Gateway transforms telecoms networks into active shields rather than mere 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 threats.

The GSMA Open Gateway initiative has been introduced by various operators across several markets in the Asia Pacific region. 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 for fraud detection and prevention.

The monetisation opportunity

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, there is also a perspective that considers combating scams as 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 the GSMA Intelligence Enterprise in Focus Survey 2024, fraud prevention emerged as the most attractive use case for network APIs across various sectors (Figure 4).

Figure 4: Network API use cases ranked by importance

Q: 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

The GSMA Open Gateway can be tailored to meet the specific needs and enhance the capabilities of various industries. By customising these APIs for different industries, the GSMA Open Gateway initiative unlocks new opportunities and enhances the capabilities across various sectors. Below are some examples:

Finance: The SIM Swap API and Number Verification API assist banks and financial institutions in identifying and preventing identity theft and fraud. These APIs ensure the security of transactions and the accurate verification of customer identities.

Healthcare: The Device Location API and Quality on Demand (QoD) API 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 carrier. This streamlines the checkout process and enhances the 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.

Transportation and Logistics: The Device Status API and Verify Location API aid in tracking shipments and managing fleet operations more efficiently. These APIs 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 various 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, delivering 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 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 undoubtedly remain a top priority for governments, operators, and stakeholders within the digital ecosystem. This is essential to sustain the growth of digital services and their contribution to socio-economic progress, aligning with the digital ambitions of governments across the Asia-Pacific region. 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 positive steps in this direction, as highlighted in previous sections of this report. However, with the constantly evolving online threat landscape, there are key considerations for stakeholders moving forward.

Post-fraud support for victims

While the efforts by various stakeholders to address scams are proving effective, there are still 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, including their life savings and borrowed funds, to scams, leaving them without a livelihood. Post-fraud assistance, such as the UK's Action Fraud reimbursement programs 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 U.S. FTC indicates that 1 in 5 victims are retargeted within a year, often using stolen personal information.[xv] Recovery services, such as identity theft protection or telecom call-blocking upgrades, help mitigate these risks. Education is also essential as teaching victims how to identify red flags can reduce repeat losses.

There is a broader perspective: 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.[xvi] This surge in reports and subsequent police action has been crucial in tackling various types of fraud, including special fraud cases and scams involving social media and investment frauds. 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, while others fall victim to fraudulent “recovery scams” that promise to return lost funds. The repercussions extend to families and communities as well, eroding trust and resources.

The role of AI and other emerging technologies in addressing scams

Emerging technologies have the potential to combat scams from multiple angles. These 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 potential to enhance anti-fraud measures when properly applied.

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

In addition to AI, other emerging technologies may also aid in combating 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, although 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, thereby 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 like 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 decrease. 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 may 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 for monetising anti-scam solutions

For industry stakeholders, combating fraud serves to protect both businesses and consumers while also presenting various monetisation opportunities. The previous section discussed the potential for operators to use anti-fraud APIs in the GSMA Open Gateway to assist enterprises across different sectors. Beyond enterprise solutions, the growing need to protect consumers from scams could potential present new 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 may include advanced authentication methods such as biometric verification through APIs, the option to upgrade to enterprise-grade security features tailored to high-risk accounts, 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 currently 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 postpaid customers; these tools identify and block suspected scam calls. They also offer a premium service called Scam Shield Premium for an additional fee (approximately $5/month as part of their Protection 360 plan or standalone in some cases). This includes enhanced features like 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. Their Call Filter Plus comes with a premium charge—typically $2.99/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 their efforts to address scams, which can inconvenience users and deter advertisers. By implementing ad verification measures to eliminate fraudulent advertisements, these 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. Enhancing 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 payment service providers. These entities 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, on the other hand, have detailed user behavioural data and content analysis capabilities to identify fraudulent patterns within their systems. By integrating these datasets, a combined data advantage is achieved, providing a more comprehensive and real-time view of potential scams. This 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 the establishment of standardised protocols. This facilitates seamless information exchange and coordinated responses across platforms and networks, thereby fulfilling the need for standardised protocols and interoperability. Crucially, cross-platform threat intelligence is essential. Shared threat intelligence, including known scam tactics, fraudulent numbers, and malicious URLs, enables proactive blocking and mitigation measures.

Additionally, a key advantage of collaboration lies in the benefit of having multiple points of verification and authentication across various mediums 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, thereby reducing the overall impact of scams.

The fight against scams is ultimately a shared responsibility. Consumers expect a secure digital experience, and the reputation of both mobile operators and digital platforms depends on their ability to provide it. By adopting a collaborative approach, they can utilise 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, virtualisation and other technologies will play a crucial role in creating smart solutions across various sectors, including healthcare, urban planning, utilities, and transportation. 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, thereby generating new market opportunities. Therefore, it is 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 that breaches can have on public trust.

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 contemporary 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 utilise 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 the Asia-Pacific region 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 like "pig-butchering" romance and investment scams originating from Southeast Asia.

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

While anti-scam solutions are essential, the trade-offs between security and individual rights can raise privacy and ethical concerns. Some tools which could be used to combat scams, such as call screening, AI monitoring, or data tracking, have the potential for overreach or could be subject to exploitation. For instance, whilst apps with the capability to analyse caller patterns or extract names, numbers, and even behavioural data from users' phones could aid in identifying scammers, they could also pose privacy risks and encompass inadequate data storage, access, and retention duration policies. A 2023 report by Privacy International highlighted certain anti-scam tools share which information with third parties, including advertisers, without obtaining explicit consent.[xvii]

Additionally, AI-driven scam filters can sometimes incorrectly flag legitimate calls, such as those from a doctor's office or small businesses, based on unreliable heuristics. A surge in the US Federal Communications Commission complaints in 2022 revealed that robocall blocks occasionally impacted nonprofits or elderly users the most, disconnecting them from essential services.[xviii] These false positives not only cause inconvenience but can erode trust and penalise innocent parties while scammers continue to adapt.

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 shares 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, 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 any 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. The formation of cross-functional working groups and a community is 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.

[i] https://www.gasa.org/research
[ii] https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf
[iii] https://www.csis.org/analysis/cyber-scamming-goes-global-unveiling-southeast-asias-high-tech-fraud-factories
[iv] GASA. (2024). Global State of Scams Report 2024
[v] https://www.hindustantimes.com/india-news/india-lost-over-rs-11-000-crore-to-cyber-scams-in-first-9-months-of-2024-report-101732716575572.html
[vi] https://opengovasia.com/2025/01/22/thailand-online-safety-awareness-and-cybersecurity-efforts/
[vii] UN. (2023). https://www.ohchr.org/en/press-releases/2023/08/hundreds-thousands-trafficked-work-online-scammers-se-asia-says-un-report
[viii] https://www.police.gov.sg/-/media/B560DF9AB68441A0B5AEAEEEF9ADCB6A.ashx
[ix] https://www.nationthailand.com/news/general/40046637
[x] https://www.ftc.gov/news-events/news/press-releases/2024/02/nationwide-fraud-losses-top-10-billion-2023-ftc-steps-efforts-protect-public
[xi] https://coinlaw.io/digital-payment-fraud-statistics/
[xii] https://www.consumerfinance.gov/about-us/newsroom/cfpb-orders-operator-of-cash-app-to-pay-175-million-and-fix-its-failures-on-fraud/
[xiii] https://www.accc.gov.au/media-release/scam-losses-decline-but-more-work-to-do-as-australians-lose-27-billion
[xiv] https://thefinancialanalyst.net/2024/11/05/gsma-and-uk-finance-launch-scam-signal-to-combat-app-fraud-in-the-uk/
[xv] https://www.ftc.gov/news-events/data-visualizations
[xvi] https://www.asahi.com/ajw/articles/15615853
[xvii] https://privacyinternational.org/long-read/5294/key-highlights-our-results-2023
[xviii] https://incompliancemag.com/fcc-issues-annual-robocalls-report/