GSMA

United Against Scams

Stand Together. Protect Together.

March 2026

Scam prevention is a global industry priority and GSMA is actively promoting a coordinated, cross-sector approach to tackling the issue. This document provides an overview of the role of mobile operators and highlights the need for public–private collaboration and innovation-led solutions alongside consumers education awareness campaigns and effective reporting.

The challenges we face

- Societies are confronting a global, growing and constantly evolving threat.
- Digital crime has expanded at an unprecedented scale, estimated to reach US$43.7 billion globally by 2028 and it now rivals or exceeds the drug trade, yet has far lower operational risks and exponentially greater growth potential due to the use of technology.
- Scam perpetrators operate across borders instantly causing colossal financial losses and individual distress worldwide, creating a major societal problem that demands urgent attention and calls for coordinated action.
- Scammers continuously outpace new anti-scam defences and regulatory responses through sophisticated technologies and techniques. They exploit jurisdictional gaps by moving between countries, identifying and exploiting vulnerabilities across the ecosystem, harnessing AI at scale attacks and adapting in real-time to circumvent newly deployed safeguards.
- No one is immune — scammers target individuals across all ages, education levels, sectors, and income brackets, making this truly a global crisis affecting hundreds of millions of people across the globe.
- Digital crime is perpetrated in many ways across different platforms operated by different entities throughout the digital ecosystem. Addressing digital crime requires all stakeholders to play their part.
- In many markets, fragmented national regulations, privacy rules and multiple regulatory authorities, legacy telecom frameworks, and inconsistent approaches limit the ability of the ecosystem participants to respond quickly and effectively against fraud. Overly prescriptive or sector-specific regulation can unintentionally slow response times, restrict responsible data sharing and reduce the flexibility needed to counter scams that evolve faster than regulations.
- Existing regulatory frameworks often lack the agility required to allow industry to adapt to the rapidly changing nature of threats presented by AI-driven attacks, which can generate sophisticated scams at scale and evolve their tactics in near real-time.
- Enforcement is also constrained by limited resources, weak coordination and the absence of harmonised cross-border legal frameworks and mechanisms that enable timely investigations, information sharing and coordinated action.
- Effective prevention and response therefore require cross-border and cross-sector collaboration, with solutions that can adapt as scammers evolve their techniques, ensuring that citizens remain safe in their daily digital lives.

1. Mobile industry leadership

1.1. Industry commitment and expertise

- Mobile operators are committed to protecting our customers and determined to take decisive action against fraud and scams.
- We stand with others on the frontlines fighting scams, investing heavily in cutting-edge defences and operating round-the-clock to protect billions of users worldwide.
- Building on years of experience combating numerous and complex threats, we have established a comprehensive security environment that continuously adapts to new threats and tactics.
- Operators share threat intelligence with each other and external partners (including banks and online platforms) to improve scam detection. Initiatives like the GSMA's Scam Signal and Open Gateway APIs help operators provide real-time signals to the financial services industry to prevent fraud losses.
- However, we cannot win this fight alone. Effective scam prevention requires proportionate responsibility across the ecosystem, aligned to each participant's technical control and visibility, and underpinned by sustained collaboration between all actors involved.

1.2. The role of mobile network operators

- Mobile operators' primary focus is on providing connectivity to a vast number of customers across the ecosystem. While the use of mobile operators' networks may serve as an entry point for a scam, the fraudulent activity takes place in other parts of the ecosystem (e.g. the approval of a payment transaction), beyond the visibility or control of operators.
- Mobile operators, within relevant legal and regulatory limits, take responsibility for the areas they directly control, including network level filtering, traffic analysis, and customer warnings. In addition, mobile operators often collaborate with third parties, including analytics engines to offer consumers and enterprises anti-impersonation services that impede fraudulent activity.
- Other participants in the ecosystem are responsible for addressing risks within their own domains—ensuring joint action as a scam unfolds—from the initial customer contact through to funds leaving a bank account. Combatting fraud is dependent on combined efforts across stakeholders involved in different aspects of the chain of events.
- Scams are executed across a range of services and technologies, not just traditional mobile messaging and voice services, but increasingly internet-based communications platforms, social media, digital payments, and digital platform environments.
- Although sustained efforts have improved spam detection and prevention on mobile networks, malicious actors are migrating to other communications platforms, attracted by lower entry barriers, encrypted environments, and their cross-border nature. This shift underscores the need for a technology-agnostic, ecosystem-wide approach to trust and safety, that encompasses all stakeholders in the scam delivery chain.
- It is therefore important that stakeholders understand what mobile operators can and cannot technically control—and take into account the technical and legal constraints operators face—when considering the most effective actions and defences for industry players across the ecosystem.
- Effective outcomes depend on shared accountability among all ecosystem participants whose systems may be exploited to facilitate scam activities. As a core principle, responsibility for scam prevention must be proportionate to technical controls and visibility across the scam delivery chain.

2. Collaboration across the value chain

2.1. We all have a part to play

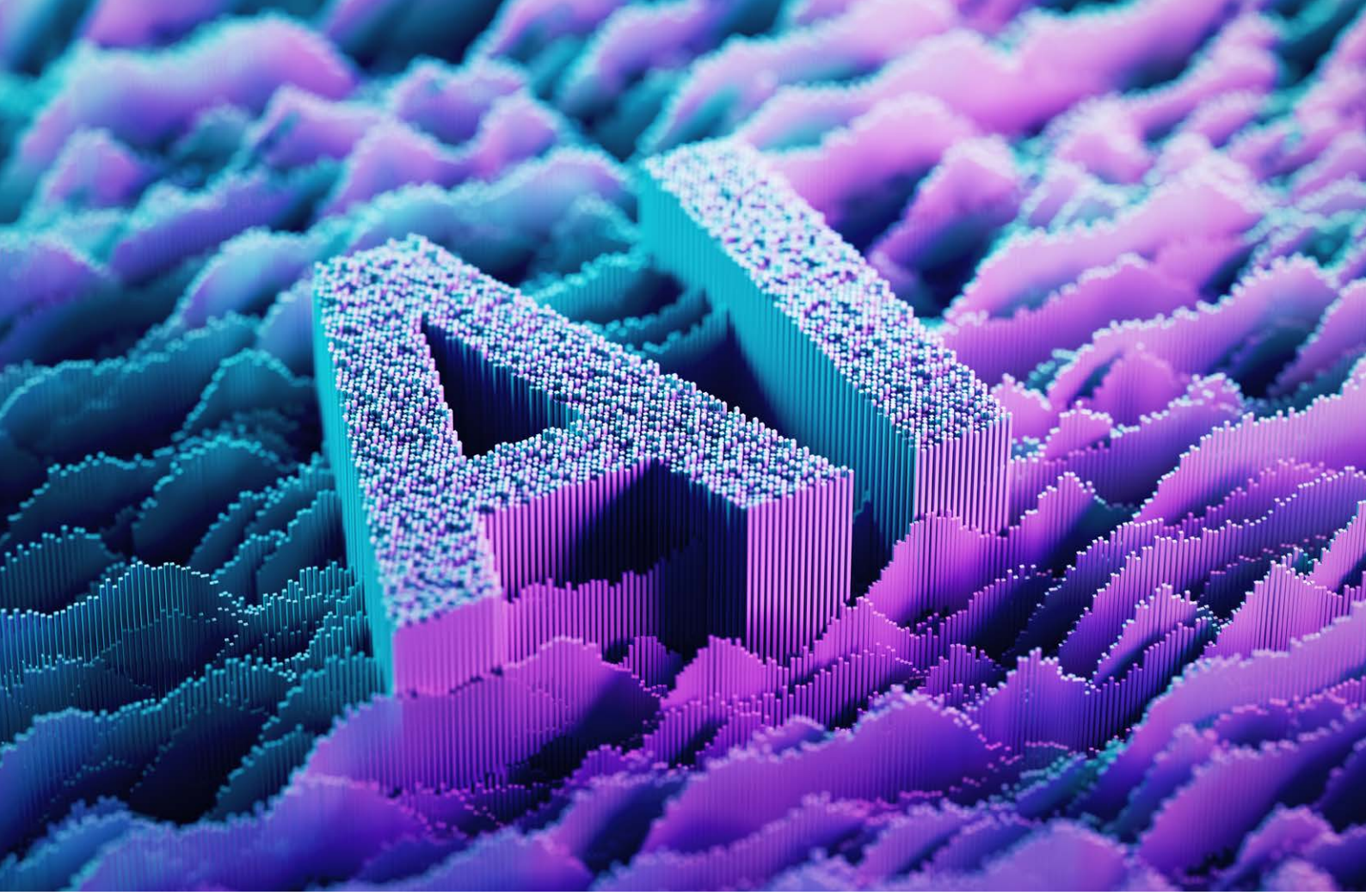
- The digital ecosystem is highly interconnected, global and complex.
- Scammers succeed by exploiting vulnerabilities across multiple services, providers and intermediaries across the delivery chain, often a combination of MNOs, digital platforms, messaging services and payment systems.
- This means successful fraud prevention requires a continuous and concerted effort across the entire value chain.

2.2. Industry's continuous and concerted effort

- GSMA Fraud and Security Group (FASG) plays a central industry-coordination role on scams, bringing together operators, vendors, and security experts to prevent, detect, and respond to scams consistently worldwide.
- Mobile operators are working in close collaboration with each other and with the GSMA to share insights and expertise while continuously investing in innovative solutions (including AI-driven technologies).

2.3. Public-private collaboration

- We are already engaged in numerous cross-sector cooperation initiatives and actively support such collaboration, recognising it as essential to effectively combatting scams.
- Collaboration between MNOs, device manufacturers, payment service providers, digital platforms and public authorities has demonstrated clear benefits in disrupting scam activity.
- Experience shows that collaboration is most effective when it is operational. For example, information sharing and near real-time coordination mechanisms should be supported by clear legal guidance that allows ecosystem participants to act quickly and in good faith.
- Interoperability should also be recognised as a critical enabler in combatting fraud, as it allows seamless data exchange between diverse fraud detection systems. This enables faster response times, higher-quality intelligence, and scalable cross-border cooperation across the ecosystem.
- It is essential to provide MNOs with legal certainty regarding the types of data they are permitted to use in combatting fraud. This clarity significantly improves the speed at which operators can deploy countermeasures within the parts of the fraud chain of events they are able to influence.
- Public authorities should duly consider the roles of the various players in the chain and prioritise collaboration between ecosystem participants—including payment service providers, electronic communication service providers and digital platforms while ensuring alignment across all administrative levels.
- We urge regulators to actively establish and champion cross-sector and public-private anti-scam initiatives, ensuring alignment and coordinated action across the entire value chain.
- A structured mechanism for sharing regulatory approval experiences across markets would accelerate the global deployment of proven anti-fraud measures.



3. Innovation

- Fraudsters are becoming increasingly sophisticated, constantly adapting their techniques and strategies to avoid new defences, technical safeguards, and regulatory measures.
- While AI-driven, real-time analysis and other technological innovations may enable new types of fraud and threats, they also provide essential tools for developing more effective anti-fraud solutions.
- Mobile operators continue to invest significant resources in identifying, filtering and blocking fraudulent traffic on their networks.
- However, there is no one-size-fits-all approach, as markets and solutions vary significantly. Mobile operators face different fraud patterns, regulatory environments, and technical capabilities across regions, requiring tailored responses. Consequently, operators are deploying diverse anti-fraud measures—both independently and through cross-sector partnerships—at varying stages of maturity and sophistication.
- Regulatory barriers may hinder progress. Legal uncertainty and legacy telecoms regulations create significant barriers in many markets, slowing the adoption of effective solutions—while scammers face none of these constraints.
- Regulators should collaborate to review existing rules, identify and remove regulatory barriers, and focus on enabling innovation to combat fraud—rather than imposing prescriptive rules that inevitably lag behind rapidly evolving fraud techniques.
- Supportive regulatory frameworks should be proportionate, flexible, and principles-based, facilitating responsible data use and intelligence sharing.

4. User education and reporting

- Educating consumers, fostering vigilance and helping people recognise warning signs remain essential defences against scams. However, long-term resilience requires more than awareness alone—it depends on building strong cyber literacy: the skills and confidence individuals need to identify, evaluate and respond effectively to evolving digital threats.
- Government-led and industry-wide awareness campaigns, supported by practical, consumer-focused fraud-prevention tools, play a vital role in strengthening this digital resilience. When consumers understand how scams operate, how trust can be manipulated and how digital services and transactions work, they are better prepared to make informed decisions and reduce their exposure to harm. In this way, informed and digitally capable consumers become a crucial line of defence alongside technical safeguards and regulatory measures.

Education efforts must be complemented by simple, trusted, operational and accessible reporting mechanisms. Effective reporting ensures that consumer reports are translated into actionable intelligence, shared insights and faster disruption of scam activity across sectors.

- Effective reporting should focus on aggregated, anonymised, non-personal data that provides actionable insights and can be shared nationally and across borders. Examples are scam typologies/categories, delivery channels, trends or shifts in behaviour, indicators of compromise, threat patterns, volume of scams, order of magnitude loss, response effectiveness metrics, cross border coordination signals, etc.

- Scam prevention cannot be achieved by any single sector, nor through isolated or prescriptive measures. It requires coordinated action across borders and industries, proportionate responsibility aligned with technical controls, and enabling policy frameworks that support innovation, responsible data use, and effective operational collaboration across the broader digital ecosystem.

We are taking action, working round the clock, sharing intelligence and best practices.

Join us: we must all be United Against Scams.

Call to Action

While solutions must be tailored to local contexts, governments and policymakers worldwide should prioritise the following measures:

1. Foster wide ecosystem collaboration

Scams exploit gaps between sectors—including telecommunications, financial services, technology platforms, law enforcement and regulators.

- Policymakers should facilitate collaboration mechanisms that enable faster intelligence sharing, earlier and coordinated responses, and formal frameworks for public-private partnerships capable of operating at the speed at which scammers evolve.
- This requires close international collaboration, including regional and international intelligence sharing mechanisms and consistent enforcement cooperation to eliminate safe havens for scam activity.

We all have a part to play.

Only by working together can we succeed.

We must all be United Against Scams.

2. Incentivise sustained innovation over regulation

The scam industry invests heavily in new technologies and continually evolves its attack methods.

- Policymakers should promote regulatory sandboxes that support rapid testing of innovative solutions and encourage collaborative frameworks with technology innovators.
- As appropriate, regulators should seek to remove barriers that prevent mobile operators from deploying anti-fraud technologies and encourage cross-sector and public-private investments.
- A flexible, principles-based policy approach is more effective than prescriptive rules that can quickly become obsolete in the face of fast-evolving fraud techniques.

3. Promote consumer education and effective reporting

Scams exploit gaps between sectors—including telecommunications, financial services, technology platforms, law enforcement and regulators.

- Governments should promote sustained educational initiatives that systematically build digital literacy, resilience and foster a culture of vigilance against evolving scam threats.
- Education efforts must be complemented by simple, trusted, and accessible reporting mechanisms that transform consumer reports into actionable intelligence. Effective reporting systems enable rapid information sharing and faster disruption of scam activity across sectors and borders.

GSMA Head Office
One Angel Lane,
London,
EC4R 3AB,
United Kingdom
gsma.com