Preventing online and ICT-enabled fraud

Best practices and recommendations for government and industry

Policy paper

ICC

Contents

Executive summary

Online fraud and fraud enabled by information and communications technology (ICT) has escalated into one of the fastest-growing and most pervasive forms of transnational crime. Online fraud and ICT-enabled fraud undermine trust in digital services, impose significant economic costs and harm individuals and communities worldwide.

What were once isolated scams have evolved into industrial-scale operations driven by organised criminal groups. These groups exploit digital technologies, global connectivity and regulatory fragmentation to target victims across borders at unprecedented scale.

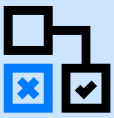
These fraud schemes increasingly rely on sophisticated social engineering, data exploitation and abuse of digital and communications infrastructure. They frequently make use of deceptive online identities, fraudulent advertising and the misuse of trusted brands and digital content to create a false sense of legitimacy and reach victims at scale. Organised criminal networks operate across jurisdictions, leveraging malware, compromised digital identities, fast payment systems and global financial channels to execute and launder fraud proceeds. The resulting harm extends far beyond direct financial losses, causing emotional distress, eroding public confidence in digital services and chilling participation in the digital economy.

Legitimate businesses across sectors, including financial services, telecommunications, digital and social media platforms, cybersecurity providers and others, are investing heavily in measures to prevent, detect, and disrupt fraud. These efforts include technical measures, advanced authentication tools, fraud detection driven by artificial intelligence (AI), controls to prevent abuse of advertising and distribution channels, consumer education and cross-industry intelligence sharing. However, no single company or sector has the visibility, authority or reach to counter transnational fraud networks alone.

In many jurisdictions, fragmented and misaligned regulatory frameworks place disproportionate responsibility on legitimate actors while failing to meaningfully disrupt the criminal organisations orchestrating fraud at scale. Divergent national rules, unclear legal frameworks and barriers to cross-border cooperation weaken collective defences and reduce the effectiveness of both public and private action.

A coordinated, internationally aligned response is urgently needed. Preventing online and ICT-enabled fraud requires elevating fraud as a priority for global cooperation, strengthening cross-border law enforcement collaboration and intelligence sharing, promoting coherent and interoperable policy approaches and expanding operationally meaningful public-private partnerships. Embedding the full range of relevant expertise across sectors can further strengthen collective efforts. Only through sustained, outcome-focused cooperation can governments and industry protect citizens, enable resilient digital economies and effectively counter organised criminal groups.

This paper highlights good practices and successful initiatives across multiple sectors and outlines key recommendations for governments and industry to strengthen the global response to online and ICT-enabled fraud:



1. **Go cross-border by default:** Fraud is transnational – enforcement must be too. Governments should strengthen international legal cooperation, streamline cross-border data access and run joint investigations targeting criminal networks.

2. **Invest in prevention, not just response:** Make scam prevention a national priority with dedicated funding, modernise data and analytical capabilities, build specialised law enforcement skills and enhance fraud intelligence capacity.

3. **Fix legal and regulatory fragmentation:** Governments should clarify laws, enable fraud reporting and intelligence sharing, support responsible AI for fraud detection and provide liability protections for companies acting in good faith. Aim for globally interoperable regulations across consumer safety, cybersecurity, privacy and data protection to reduce legal ambiguity and encourage proactive prevention.

4. **Operationalise public–private cooperation:** Move beyond dialogue to real-time operational collaboration, including joint operations cells, trusted intelligence-sharing platforms and coordinated public education campaigns. Encourage cross-industry and multilateral collaboration to prevent fraud before it happens.

Governments, industry, law enforcement agencies and civil society must work together to strengthen cross-border enforcement, align regulatory approaches and expand operational public-private partnerships. These efforts should aim to disrupt organised criminal groups, protect individuals and businesses and reduce unnecessary regulatory burdens, focusing resources on **the core objective: stopping fraud at its source**.

1. Scale and drivers of online and ICT-enabled fraud

1.1 Defining the landscape

Online and ICT-enabled fraud is any form of deception that utilises digital technologies, Internet-based tools or information and communication technologies, or exploits human behaviours to illicitly acquire money, property or sensitive information from an individual or organisation.

Unlike traditional theft, online fraud is fundamentally rooted in deception and social engineering. It is distinguished by the use of technology to expand the scale and reach of traditional crimes, allowing perpetrators to operate remotely and with a degree of anonymity. It often relies on the deliberate imitation of trusted services, brands or digital environments to appear legitimate. It is fundamentally about tricking victims into voluntarily providing assets or data. The methods are constantly evolving and are not tied to any single industry, impacting individuals and businesses across all sectors.

The core categories outlined in **Table 1** – impersonation scams, phishing, account takeover, business e-mail compromise, tech support fraud, online marketplace fraud, telecom fraud and malware-enabled fraud – often overlap in practice. A single fraud campaign may combine phishing to harvest credentials, the replication of familiar interfaces or branding to build trust, malware to maintain persistence, impersonation to manipulate victims and fast payment rails to move funds before detection.

These blurred boundaries complicate traditional distinctions between cybercrime, financial fraud and consumer scams. What may begin as a social engineering attack frequently relies on underlying cybercrime techniques, exploits financial infrastructure and abuses communications networks simultaneously. As a result, effective prevention and enforcement require integrated, cross-sector responses rather than siloed approaches.

Table 1: Core categories of online and ICT-enabled scams and fraud

Category	Description
Impersonation scams	Scammers pose as trustworthy individuals or entities, such as government officials, relatives, or representatives from well-known companies to trick victims into providing money or personal information.
Phishing	This involves the use of deceptive emails, text messages or websites that appear to be from legitimate sources to lure victims into revealing sensitive data like passwords and credit card numbers.
Account takeover	Scammers gain unauthorised access to a user's online accounts, such as e-mail or social media, to steal personal information or commit further fraud.
Business e-mail compromise	Scammers target businesses by sending emails that appear to come from a known source, such as a CEO or a vendor, to request a fraudulent payment or sensitive data.

Category	Description
Tech support fraud	Scammers pose as technical support representatives from well-known companies and use fear tactics to convince victims that their computers have a serious problem that needs to be fixed for a fee.
Online marketplace fraud	Deceptive practices occur on online platforms where goods and services are sold, including the sale of counterfeit goods, non-delivery of items and payment scams.
Telecom fraud	Telecom fraud involves the misuse of telecommunication systems and networks for deceptive practices to steal money or avoid charges.
Malware-enabled fraud	Malicious software (malware) is used to infect devices, allowing criminals to steal personal information, disrupt computer systems or hold data for ransom.
Fake adverts on social media	Scammers create deceptive ads or promotional posts to trick users into giving away money, personal information or account access. These scams often look legitimate and are designed to blend in with normal ads or influencer content.
Romance scams	Romance scams are a form of social engineering where a criminal builds trust with their intended victim, eventually persuading them to make a financial transaction, often into a fake account.

1.2 Evolution and sophistication of fraud tactics

The methods employed by malicious actors in online and ICT-enabled fraud are in a state of constant evolution, moving far beyond the simplistic scams of the past. Today's fraudulent activities are characterised by a high degree of technical sophistication, strategic organisation and rapid adaptation, presenting formidable challenges for businesses, governments and consumers alike.

A primary driver of this sophistication is the weaponisation of new technologies to create deception at an unprecedented scale. The widespread availability of generative AI, for instance, has been exploited by criminals to craft highly convincing fraudulent content, from phishing emails with flawless grammar to realistic synthetic media (that is, "deepfakes") for impersonation. This technology is paired with the automation of social engineering, enabling fraudsters to deploy millions of personalised scam messages across e-mail, SMS and social media with minimal effort. This reality underscores the critical importance of deploying equally sophisticated, AI-driven defence mechanisms. Just as attackers use AI to scale their operations, organisations must leverage AI to detect and neutralise these advanced threats at a scale and speed that human moderation cannot match.

This evolution is supported by a maturing and professionalised cybercrime ecosystem. The emergence of Malware-as-a-Service (MaaS) and Fraud-as-a-Service (FaaS) models has lowered the barrier to entry, providing aspiring criminals with access to sophisticated tools, infrastructure and expertise on a subscription basis. These illicit marketplaces facilitate the trade and use of compromised or spoofed digital identities – such as e-mail accounts, social media profiles and government-issued digital IDs – which have become a cornerstone of modern fraud. By leveraging these services, attackers can impersonate individuals and organsations with a high degree of authenticity to execute complex schemes, like account takeover and business e-mail compromise.

Furthermore, fraudsters demonstrate a remarkable ability to adapt to new security measures across the digital ecosystem. This is evident not only in the financial sector, where they develop innovative techniques to target faster payment systems and cross-border transactions, but also across major online platforms. On social media, e-commerce sites and other digital services, criminals continuously probe for and exploit vulnerabilities in trust and safety mechanisms. This continuous cat-and-mouse game, where new security controls are quickly analysed and circumvented, proves that static defences are no longer sufficient. To effectively combat fraud, organisations must adopt a dynamic, intelligence-led approach, constantly monitoring for new threats and adapting their defences to counter an adversary that is always learning.

1.3 Role of organised crime groups

The origin of the industrialised criminal model is rooted in the strategic adaptability of transnational organised crime groups (TOCs). Before the COVID-19 pandemic, certain criminal groups invested billions in gambling infrastructure (for example, large casinos and hotels) across Southeast Asia.[1] When pandemic-related lockdowns and border restrictions halted the flow of tourists and gamblers, gambling profits collapsed. These TOCs, demonstrating exceptional business agility, repurposed their existing facilities into high-tech "fraud factories" to secure new revenue streams. This shift substituted casino customers with global online scam victims, allowing the criminal networks to maintain and even accelerate profitability.[2]

Highly sophisticated and organised: The sophistication of these operations stems from the high degree of organisation exhibited by the TOCs managing them. TOCs, particularly those based in Southeast Asia, have adopted the identity of "criminal service providers", offering a wide, convergence-based portfolio of illegal activities, including fraud, human trafficking and money laundering.[3]

Transnational operations: A striking complexity in the operational blueprint of TOCs is the their strategy of global sourcing and cross-market targeting. Scam centres often internally segregate workers by language – for example, housing Vietnamese workers to target the Vietnamese market or Chinese-speaking workers targeting China.[4] By recruiting victims from over 100 countries and simultaneously targeting multiple markets worldwide, TOCs diversify their revenue streams and strategically avoid over-reliance on a single jurisdiction. This strategy makes isolated national-level crackdowns inefficient as disruption in one country simply accelerates the relocation of a TOC or focus on less cooperative target markets, underscoring the necessity for internationally coordinated legal and law enforcement action.

Combined with other types of crime, including violent crime, human trafficking and money laundering: This model highlights the poly-criminal nature of the threat. Financial fraud is no longer isolated but is intrinsically linked to violent crime, human trafficking and sophisticated money

1 CSIS, "Cyber Scamming Goes Global: Sourcing Forced Labor for Fraud Factories," accessed October 23, 2025, https://www.csis.org/analysis/cyber-scamming-goes-global-sourcing-forced-labor-fraud-factories
2 Ibid.
3 CSIS, "Cyber Scamming Goes Global: Unveiling Southeast Asia's High-Tech Fraud Factories," accessed October 23, 2025, https://www.csis.org/analysis/cyber-scamming-goes-global-unveiling-southeast-asias-high-tech-fraud-factories
4 UNODC, "Southeast Asia and the Pacific Organized Crime Threat Alert," accessed October 23, 2025, https://www.unodc.org/roseap/uploads/documents/Publications/2025/UNODC_Alert_Strategic_infiltration_of_vulnerable_jurisdictions_through_criminal_foreign_direct_investments.pdf

laundering infrastructure.[5] The resilience of TOCs means that disruption efforts targeting only one illicit revenue stream (for example, drug trafficking or illegal gambling) will merely accelerate their diversification into other service-based criminal models, such as industrial-scale cyber-fraud or money laundering-as-a-service. This convergence elevates cyber-enabled fraud beyond a mere economic issue, making it a pivotal strategic threat vector.

Clear geographic patterns have emerged in the operations of transnational scam networks. Investment fraud, in particular, is estimated to be carried out by organised crime groups in approximately 69–70% of cases, highlighting the dominant role of structured criminal organisations rather than isolated individuals.

A limited number of countries in Southeast Asia and parts of Africa have become major hubs for scam activity, where key infrastructure, coordination centres and so-called "scam compounds" are often based (**Table 2**). From these locations, transnational organised crime networks conduct fraud campaigns that target victims worldwide, deliberately operating across borders to take advantage of jurisdictional gaps and uneven enforcement environments. Many of these operations are associated with the use of forced labour within scam compounds, adding a severe human and social dimension to the financial harm inflicted. Syndicates operating from countries in the Mekong region alone are estimated to have stolen over US$43.8 billion globally, illustrating the scale, sophistication and reach of these criminal networks.[6]

Table 2: Transnational organised crime (TOC) hubs and operational convergence
(as of October 2025)

TOC hub region	Key locations / compounds	Primary TOC actors	Defining characteristics	Primary scams hosted
Southeast Asia	Myanmar (KK Park, Shwe Kokko), Cambodia (Sihanoukville, Bamban), Laos, Philippines	Chinese-speaking syndicates, Prince Group TOC, Yakuza-affiliates, Myanmar ethnic armed organisations (EAOs)	Forced labour camps, exploitation of special economic zones (SEZ), conflict financing (Myanmar), criminal foreign direct investment (FDI)	Cryptocurrency investment fraud, pig butchering, romance scams
West Africa	Ghana, Nigeria, Côte d'Ivoire, Namibia	West African crime groups (TOCs)	Globalised forced labour (Namibia, for example), transnational operations (21 countries)	Romance fraud, investment fraud, advance fee fraud, business email compromise (BEC)

5 Amnesty International, "Cambodia: Government Allows Slavery and Torture to Flourish Inside Hellish Scamming Compounds," accessed October 23, 2025, https://www.amnesty.org/en/latest/news/2025/06/cambodia-government-allows-slavery-torture-flourish-inside-scamming-compounds/

6 USIP, "Transnational Crime in Southeast Asia", accessed March 4, 2026, https://www.usip.org/sites/default/files/2024-05/ssg_transnational-crime-southeast-asia.pdf

TOC hub region	Key locations / compounds	Primary TOC actors	Defining characteristics	Primary scams hosted
South Asia	India (Delhi-National Capital Region, various cities)	Organised call centre syndicates	Vishing specialisation (voice phishing), impersonation of US / UK authorities, resembles legitimate business process outsourcing (BPO)	IRS / social security scams, tech support scams, loan fraud

2. Industry efforts and best practices

2.1 Cross-industry initiatives

Industry actors across sectors have recognised that fraud prevention requires collective action. Voluntary collaboration initiatives aim to protect consumers, secure digital ecosystems and disrupt organised crime by sharing intelligence, aligning practices and reducing abuse of digital and communications infrastructure. These efforts increasingly draw on a wide range of tools, including established mechanisms to identify and address impersonation and deceptive misuse of trusted digital assets, as well as the exchange of operational intelligence that can reveal coordinated fraud activity across channels and services.

Shared goals include enhancing fraud intelligence sharing, identifying emerging threats and coordinating responses across platforms, networks and financial systems. Examples include cross-sector taskforces, information-sharing alliances and joint technical initiatives supported by industry associations and multilateral partners.

In practice, this also involves using existing reporting and takedown channels to detect and remove fraudulent content, fake storefronts, misleading advertisements and impersonation attempts across platforms, marketplaces and domain ecosystems. There is growing recognition of the value of sharing more granular indicators, such as behavioural fraud signals, recurring brand impersonation patterns, clusters of machine-generated spoofed domains and infrastructure linked to malware-as-a-service operations.

Cross-industry initiatives illustrate a clear shift toward coordinated, cross-sector responses to online fraud that go beyond isolated enforcement efforts:

- They demonstrate the growing importance of **cross-industry intelligence sharing**. Platforms such as the Global Signal Exchange (GSE) and the Asia Pacific Cross-Sector Anti-Scam Taskforce (ACAST) are examples of cross-industry information sharing aimed at tackling fraud and scams. Another example is the case of Spain, where telecom mobile operators proactively engage with banks to monitor fraud and prevent SMS spoofing, including procedures to prevent spoofing via application to person (A2P) SMS platforms.
- They also show the value of **global coalitions spanning multiple sectors**. The Global Anti-Scam Alliance (GASA) brings together major technology firms, financial institutions, telecom operators, consumer protection bodies and regulators under a shared mission to prevent scams and protect consumers, creating a common forum for coordination and collective action.
- They bring **innovative technical solutions**. For example, the GSMA Open Gateway enables mobile operators to share network intelligence with trusted partners, including banks, fintech and digital platforms, in a secure way to prevent fraud.
- Furthermore, these efforts highlight **active government participation alongside the private sector**. Public authorities such as Singapore's GovTech are not only endorsing cooperation but directly integrating into joint intelligence-sharing platforms, helping to bridge long-standing public-private divides in fraud response. Another example is the UK with its Joint Fraud Taskforce (JFT), chaired by the Home Office's Minister responsible for fraud prevention, which is a partnership between the private sector, government and law enforcement to tackle fraud collectively. It has led to the formation of a multi-agency, public-private partnership that

is seeking to create new cross-sector data sharing capabilities and look for opportunities to design out fraud.

- These cooperative efforts help **transnational law enforcement**. For example, the SimCartel operation, led by Europol in cooperation with different member states and the private sector, dismantled a cybercrime-as-a-service network behind thousands of online frauds across Europe.[7]
- Finally, they underscore the role of **multilateral reinforcement**. Organisations such as the United Nations Development Programme (UNDP) are providing practical handbooks and guidance that translate high-level commitments into operational frameworks, enabling governments, companies and civil society to align their actions against scams.

Together, these examples show that while law enforcement capacity alone has struggled to keep pace with the growth of fraud, structured public-private and multilateral collaboration is emerging as a critical force multiplier.

2.2 Practical best practices

Prevention

Businesses deploy a range of preventive measures, including user education campaigns, digital solutions, advanced authentication and identity verification, platform integrity rules and proactive risk detection. A growing focus is being placed on strengthening the identity and sender layer across the digital ecosystem, recognising that many fraud schemes exploit weak or spoofed identities rather than technical vulnerabilities alone.

AI-enabled fraud detection models play a growing role, allowing defenders to analyse vast datasets, identify patterns and respond in real time. Leading industry actors are increasingly deploying responsible AI systems designed specifically to counter emerging AI-enabled fraud threats, including the detection of voice cloning, synthetic identities and deepfake-driven impersonation attempts. Initiatives such as the GSE demonstrate how AI and machine learning can support cross-sector intelligence sharing at scale, while VMO2's Daisy, the "AI granny" project demonstrates how AI can also be used for awareness-raising and combatting scams.[8]

Preventive identity-layer safeguards increasingly include verified sender and account trust frameworks. These include domain-based message authentication and validation mechanisms that help reduce spoofed emails and messages, multi-factor verification for high-risk account actions and "verified business" indicators that help users distinguish legitimate entities from impersonators. By reinforcing trust signals at the point of interaction, these measures reduce the effectiveness of social engineering and impersonation-based scams.

Network analysis and data sharing on known fraud vectors, when enabled by regulation, facilitate earlier detection and disruption of coordinated campaigns. Sharing indicators, such as malicious URLs, IP addresses, phone numbers and wallet addresses helps prevent re-use across platforms. Machine learning models are also being used to detect brand impersonation at scale, flagging unauthorised use of trademarks, logos, user interface mimicry and other graphical elements commonly exploited in scams and fraudulent advertising.

---

7 Europol, "Cybercrime Service Takedown: 7 Arrested," accessed October 23, 2025, https://www.europol.europa.eu/media-press/newsroom/news/cybercrime-service-takedown-7-arrested

8 Virgin Media O2, "O2 Unveils Daisy: The AI Granny Wasting Scammers' Time," accessed October 23, 2025, https://news.virginmediao2.co.uk/o2-unveils-daisy-the-ai-granny-wasting-scammers-time/

The use of innovation is transforming fraud prevention from reactive response to pre-emptive protection, leveraging the scale and connectivity of mobile networks to identify threats as they emerge. For example, the GSMA Open Gateway illustrates how standardised, open-source telecom application programming interfaces (APIs) can support fraud prevention by enabling real-time access to network intelligence. This ecosystem approach, including solutions like Scam Signal, shows how innovation and cross-sector coordination can shift fraud defence from reactive response to pre-emptive protection.

Detection

While AI is being misused to produce more sophisticated scams, defenders can leverage the full power of AI to disrupt these fraudulent activities.[9] AI plays a crucial role in the fight against scams and fraud, accelerating the detection of abuse, generating insights and scaling efforts against harm across a variety of platforms. AI models that enable real-time analysis of vast amounts of data allow for the rapid identification of patterns and anomalies that may indicate clusters of fraudulent activity, including coordinated impersonation campaigns and the reuse of deceptive brand assets across channels.

Detection capabilities are increasingly complemented by risk-based identity proofing for high-risk accounts and transactions. Practices, such as adaptive re-authentication, device trust scoring and continuous access evaluation, help identify anomalous behaviour over time and limit the ability of fraud actors to persist once access has been gained. These approaches reflect how major platforms, cloud providers and financial institutions assess trust dynamically rather than relying on one-time verification alone.

The GSE platform is also evolving to utilise machine learning algorithms to continuously improve its ability to detect and predict new and evolving scam campaigns. As AI continues to evolve, ICC expects it to play an increasingly important role in safeguarding users and platforms from fraudulent activities. AI-powered enhancements, such as keyword AI and cluster analysis machine learning models, are transforming capabilities, allowing for deeper insights into scam tactics and targeted brand threats.[10]

Disruption

Disruption efforts include takedowns of malicious infrastructure, coordinated action against mule accounts and botnets and reporting to law enforcement. Many platforms also rely on automated content integrity safeguards, including safe content pipelines that rapidly remove fraudulent advertisements, listings, cloned profiles or impersonating accounts once detected.

Where enabled by regulation, to increase speed and consistency at scale, industry is increasingly exploring automated takedown integrations, such as API-based reporting of malicious domains, counterfeit applications and impersonating content; standardised abuse reporting formats; and clearer service-level expectations with registries, hosting providers and other infrastructure operators. When combined with strengthened identity controls and shared intelligence, these measures reduce criminals' ability to rapidly reconstitute operations across platforms.

---

9 Google, "How AI Can Reverse the Defender's Dilemma," accessed October 23, 2025, https://services.google.com/fh/files/misc/how-ai-can-reverse-defenders-dilemma.pdf

10 Google, "Leveraging AI through the Global Signal Exchange to Tackle Scams," accessed October 23, 2025, https://static.googleusercontent.com/media/publicpolicy.google/en//resources/ai_responsibility_and_scams_gse_en.pdf

Proactive tracking and disruption of fraud supply chains – such as dismantling phishing kit distribution networks, blocking large clusters of scam domains using AI clustering and coordinating with banks, fintechs and crypto analytics providers to address mule accounts and illicit payment flows – is increasingly recognised as a best practice to prevent the rapid regeneration of fraud infrastructure.

Transparency and accountability practices further strengthen these efforts. Major global providers routinely publish annual digital safety reports, transparency reports on takedowns and threat intelligence digests. Encouraging cross-industry transparency frameworks and shared metrics on fraud prevalence, takedown speed and user risk reduction can reinforce trust, support benchmarking and enhance collective understanding of evolving threats.

Case studies (**Table 3**) – from telecom call authentication technology to financial sector transaction monitoring and cybersecurity-led infrastructure disruption – illustrate the effectiveness of coordinated action when supported by timely intelligence and clear legal authority.

Table 3. Selected case studies

Cross-sector information sharing
Global Anti-Scam Alliance (GASA) A global coalition of +100 members working with law enforcement and industry to share intelligence on scams and malware **Impact:** Enables coordinated action across banks, telecom operators, tech companies and enforcement authorities.
Global Signal Exchange (GSE) Launched in 2024 as a global clearinghouse for bad actor signals **Impact:** +800 million fraud indicators shared across 250 organisations by December 2025, accelerating cross-platform scam detection
Asia Pacific Cross-Sector Anti-Scam Taskforce (ACAST) Unites mobile operators and digital platforms across 17 countries **Impact:** Drives coordinated awareness campaigns and technical mitigation strategies across the region
GSMA Fraud and Security Group (FASG) and Telecommunication Information Sharing and Analysis Centre (T-ISAC) Global industry-led intelligence-sharing for mobile operators **Impact:** Enables the co-ordination of industry-wide fraud mitigation strategies and development of best-practice security frameworks to reduce fraud risks
Digital innovation
GSMA Open Gateway Provides standardised mobile network APIs to developers, banks and fintech **Impact:** Enables secure services such as SIM Swap detection, number verification, and device location through trusted operator network data

Scam Signal API
Developed originally UK Finance, UK mobile operators, UK banks, and GSMA
Impact: Improved detection rates of up to 40% for authorised push payment scams in the UK by analysing real-time mobile data and blocking suspicious activity before it gets to customers

Public-private collaboration

RedVDS disruption
Joint action by Microsoft's Digital Crimes Unit and US and European law enforcement
Impact: Dismantled infrastructure linked to +191,000 compromised e-mail accounts and over US$40 million in losses

GSMA Capacity-Building Programme
Supports governments, regulators and law enforcement in strengthening fraud response capabilities
Impact: Enhances institutional readiness and cross-border cooperation to tackle scams effectively

3. Recommendations for government action

1. Strengthen cross-border enforcement

- Improve international cooperation frameworks and legal processes
- Streamline cross-border data request mechanisms
- Streamline mechanisms for cross-border data requests
- Enhance operational coordination to target organised crime groups, infrastructure and financial flows

2. Increase prevention capacity

- Elevate scam prevention as a national priority with dedicated resources
- Modernise government's data capabilities and streamline reporting
- Provide training for law enforcement agencies

3. Ensure regulatory coherence and interoperability

- Enable innovation in fraud prevention and avoid fragmentation and duplicative compliance requirements for legitimate businesses
- Promote globally interoperable approaches to fraud reporting and information-sharing
- Align regulatory expectations with operational realities and risk-based frameworks
- Encourage consistent definitions of fraud types and roles/responsibilities

4. Build meaningful public-private partnerships

- Establish structured, sustained and operationally grounded cooperation channels
- Maintain real-time or near-real-time engagement models where appropriate:
- Foster trusted environments for intelligence exchange between sectors and authorities
- Prioritise outcomes
- Launch (joint) public education campaigns

3.1 Strengthen cross-border enforcement

Improve international cooperation frameworks and legal processes: Facilitating and strengthening cross-border investigations is essential so that law enforcement agencies and private organisations – like online platforms and financial institutions – can work together across borders to tackle transnational organised crime networks. The perpetrators, victims, key documents and third parties involved in the fraudulent transaction are often widely dispersed across borders, which makes it challenging for enforcement agencies and other relevant government entities in a single country to gather all the information necessary to detect scams and fraud and investigate them effectively. Stronger cooperation frameworks can also enable the more effective action against the digital infrastructure that supports fraud operations, including websites, domains and impersonating online content used to deceive victims at scale.

As one example of this type of cross-border cooperation, in 2023, the Council of the OECD adopted Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices across Borders. The guidelines recommend specific enhancements to both domestic legal and enforcement

frameworks, as well as mechanisms to facilitate notification, information sharing, assistance with investigations and confidentiality, notably across borders and in cooperation with private sector entities. For global businesses like online platforms and financial institutions, this international alignment and legal interoperability would greatly improve the effectiveness and efficiency of compliance efforts as well as private litigation.

Policymakers should explore implementing similar frameworks and collaborations, either regionally or through bodies like the OECD, to achieve better detection and enforcement against organised criminal networks and strengthen these actions in the future, especially across borders.

Streamline mechanisms for cross-border data requests: Policymakers should streamline the legal process for submitting and processing requests related to fraud investigations, ensuring that private companies can efficiently comply with lawful requests from authorities while respecting due process. In this respect, there are various possible voluntary frameworks that governments could put in place such as CLOUD Act Agreements, the Budapest Convention and more recently the Second Additional Protocol to the Budapest Convention, which establishes mechanisms for dealing with cross-border access in a manner that respects the rule of law. Specifically, ICC would encourage governments to consider signing and ratifying the Second Additional Protocol.

Enhance operational coordination to target organised crime groups, infrastructure and financial flows: Governments and regional agencies should therefore prioritise stronger operational coordination across borders, enabling law enforcement agencies to work together to target not only individual scam incidents, but the organised crime groups, technical infrastructure and financial flows that underpin large-scale fraud operations. This includes coordinated investigations, joint task forces and aligned strategies to disrupt scam compounds, digital infrastructure (such as domain takedowns and the removal of cloned or impersonating online assets where legally permitted), mule networks and money laundering channels. By focusing on the full criminal ecosystem rather than isolated events, authorities can more effectively dismantle networks and reduce their ability to rapidly reconstitute operations elsewhere.

Key takeaway

Fraud is transnational and enforcement must be too. Governments should modernise cooperation frameworks by strengthening cross-border legal and operational coordination, streamlining lawful data-sharing mechanisms and working with international partners and the private sector to disrupt organised criminal networks and the digital and financial infrastructure that enables large-scale fraud, not just individual scams.

3.2 Increase prevention capacity

Elevate scam prevention as a national priority with dedicated resources: Governments should formally declare scam prevention a national priority, akin to a national security threat. This should be accompanied by explicit budgeting for anti-scam initiatives, including increased funding for law enforcement personnel, specialised tools (for example, crypto tracing capabilities) and training for law enforcement. Diplomatic and legal measures, including criminally sanctioning / formally proscribing groups, networks and companies involved in scams and fraud, can further support disruption and the efforts of private companies to counter these entities.

Modernise governments' data capabilities and streamline reporting: Governments must urgently invest in modernising their data collection and analysis capabilities for combating financial crimes, specifically improving existing databases.

Provide training for law enforcement agencies to better investigate and prosecute cybercriminals can help strengthen enforcement and the private sector among others can help with these capacity-building efforts.

Key takeaway

Prevention must be treated as a national priority. Dedicated funding, modern data capabilities and specialised training are essential to shift from reactive enforcement to proactive disruption.

3.3 Ensure regulatory coherence and interoperability

Enable innovation in fraud prevention and avoid fragmentation and duplicative compliance requirements for legitimate businesses by considering measures, such as:

- **Deconflicting laws and providing legal clarity to enable action:** Policymakers must review and harmonise existing legal and regulatory frameworks, particularly at the intersection of consumer safety, cybersecurity, privacy, anti-fraud laws, data protection, competition rules and intellectual property to eliminate ambiguities that hinder proactive anti-scam efforts and the roll-out of innovative digital solutions at scale.
- **Fostering investment in responsible AI and policies that encourage technological innovation against scams and fraud:** There is a role for policymakers to play in ensuring that legislative frameworks allow for anti-fraud innovation and tools necessary to counter the misuse of synthetic media. The latest wave of AI innovation has the potential to revolutionise the way that governments, businesses and online platforms identify scammers and take action against fraudulent content. AI has enabled the acceleration of fraud and scam detection, scaling private sector approaches towards fighting abuse and harm across platforms. It also has the potential to help better identify and stop instances of personal data leaving networks in an unauthorised way.

  Unlocking the potential of these advanced technologies requires that policymakers, companies and civil society work together to invest in responsible AI – including the infrastructure, the workforce and the legal framework needed. At the same time, there is a risk that overly restrictive approaches might limit the ability of governments and businesses to use AI to improve fraud detection and online safety. Governments should encourage stakeholders to innovate in – and utilise – AI responsibly to combat fraud.

Promote globally interoperable approaches to fraud reporting and information-sharing: Any effective response to fraud and scams must be built on intelligence. Enhanced cooperation and lawful information sharing across industries and with law enforcement, both domestically and internationally, is critical. Governments should adopt and implement laws that facilitate the sharing of relevant, sensitive data for fraud detection and prevention while safeguarding privacy and security.

Empowering governments, private sector entities and other organisations with the information necessary to identify fraud actors, their tactics and the infrastructure that enables their activities is essential. Governments should promote globally interoperable approaches to fraud reporting and harmonised information sharing frameworks that provide regulatory clarity, incentivise reporting and complement existing sectoral processes rather than duplicate them.

Currently, a patchwork of national laws – with potentially conflicting obligations – have created a lack of clarity that disincentivises the optimal level of information sharing necessary to effectively combat fraud and scams.[11] Moreover, a lack of sufficient clarity surrounding global privacy and data protection laws has also created the perception – often incorrectly – that such laws are impediments to organisations safely sharing fraud and scam intelligence with one another and with governments.

Governments should adopt or clarify laws to facilitate cooperation and information sharing between industry and authorities. Online platforms and financial institutions should be legally authorised to act on suspicious activity, including sharing sensitive information such as account details, transaction data and other indicators with government, regional and international agencies, and vice-versa. Policymakers should ensure a clear, balanced, globally interoperable legal framework that enables responsible information sharing.

By clarifying or amending laws, governments can remove real or perceived impediments that may discourage or disincentivise private organisations from reporting or sharing intelligence with each other and with authorities. Among other approaches, governments can consider the creation of "safe harbour" limitations of liability for entities acting in good faith to share, receive or act on fraud intelligence.

Coordinated global approaches to defining what fraud-related information can be shared, with whom and under what conditions are essential to enable effective international cooperation. National and regional agencies should harmonise reporting rules and standards to create a common global architecture that empowers organistations to prevent fraud and governments to investigate perpetrators efficiently.

In some jurisdictions, it may also be necessary to clarify the intersection between consumer safety and anti-fraud laws with other legislation such as data protection and competition rules.

Align regulatory expectations with operational realities and risk-based frameworks by considering measures such as:

- **Clearly defining illegal activity in regulation and legislation:** In order for law enforcement agencies and private entities, such as online platforms and financial institutions, to take effective action against fraud and scammers, policymakers must clearly codify what constitutes illegal activity in their jurisdiction. Without this legal clarity, public and private entities may be reluctant to take decisive or preventive action. Governments should therefore review their existing legal frameworks to assess whether they are fit for purpose for fighting scams and fraud, such as privacy laws and data sharing mechanisms. If gaps are found, policymakers should look to introduce new or enhanced frameworks or issue supporting guidance to clarify how existing frameworks should be enforced. In doing so, policymakers shall consider existing regional and international standards, regulations and best practices.

11 N. Maxwell, "A New Era of Private Sector Collaboration to Fight Economic Crime," Future of Financial Intelligence Sharing (FFIS) Research Programme, March 2025.

These legal frameworks should clearly define what constitutes illegal activity in this context and include reasonable enforcement mechanisms. This is particularly important as often digital platforms are not in a position to determine what is a scam because of a lack of visibility on the overall scheme, including behaviour occurring on other platforms or offline.

- **Incentivising preventive action by stakeholders through "Good Samaritan" liability protections:** Governments can incentivise companies to take preventive action against fraud and scams through the adoption of "Good Samaritan" liability protections, which shield private organisations from liability for their proactive efforts against online harm. A good way to understand why this is important is to think about what might happen to a company if the protections are not in place. For instance, online platforms could be sued for decisions around removal of content such as hate speech, mature content or videos relating to illegal pyramid schemes. The result of these pressures would be to disincentivise companies from developing robust content moderation systems. It is important that the liability regime provides clarity and does not disincentivise services from taking positive, voluntary measures to tackle scams and other content challenges.

  A service should not become liable for any of the information that it hosts simply by virtue of the fact that it has taken voluntary action in good faith, whether of an automated or a non-automated nature. "Good Samaritan" protections would address that concern by giving protection for platforms to seek out and remove harmful content without risking the loss of liability protections for occasional failures in that process.

  Examples of legal provisions to incentivise preventive action by shielding online services from liability for their proactive prevention efforts against online harms are included in the EU Digital Services Act (DSA) and section 230 of the US Communications Decency Act (CDA). In other jurisdictions, similar protections could avoid disincentivising companies from proactively searching for fraudulent content and actors from sharing threat information.

- **Remove regulatory barriers hindering innovation:** Governments should remove regulatory obstacles that limit the deployment of anti-fraud innovation. In certain regions, fragmented implementation of regulations creates significant barriers, slowing the adoption of innovative solutions such as anti-fraud APIs. In these contexts, businesses are often required to seek prior approval from national authorities before implementing technical measures, particularly those involving data use and sharing. Governments should therefore promote proportionate, flexible and principles-based regulatory frameworks that enable responsible data use and effective intelligence sharing.

Encourage consistent definitions of fraud types and roles / responsibilities: To enable international cooperation and collaboration in the fight against fraud, national and regional law enforcement agencies, private organistations and others need to speak a common language when defining fraud and scams. For investigators to be able to effectively use fraud and scam intelligence, they need to understand the data they are receiving, what it represents and what it can enable them to do. Governments should look to emerging standards that can be leveraged to harmonise the global fraud taxonomy.

For instance, the US Federal Reserve has established two voluntary classification systems – the FraudClassifier Model and the ScamClassifier Model – that attempt to help create a common set of definitions for fraud and scams to address challenges in inconsistent classification.[12] [13]

By identifying a common standard through which public and private stakeholders and private organisations can define and classify fraud and scams, ICC can enable all organisations to better curate what information they are sharing and how it is used. With a harmonised global approach to data classification and data sharing, private organisations will be better positioned to prevent and mitigate the harm caused by fraud actors and governments will be well-positioned to investigate perpetrators with the speed necessary to meet the evolving threat.

Key takeaway

Clear, harmonised and innovation-enabling legal frameworks are critical. Policymakers must remove fragmentation, enable responsible information sharing, provide legal clarity and support technological innovation to strengthen fraud prevention at scale.

3.4 Build meaningful public-private partnerships

Establish structured, sustained and operationally grounded cooperation channels: Greater dialogue among the anti-scam community is essential, from detecting and sharing information about new threats, trends and patterns to collaboration on actual investigations. Policymakers should encourage online platforms and the private sector – particularly high-risk organisations like financial institutions – to hold regular, multi-stakeholder dialogues. Similarly, governments should join or endorse these cooperation forums to ensure close and consistent coordination across the ecosystem. This can support proactive prevention, enable quick and effective responses and help others be better prepared.

Beyond dialogue, some jurisdictions and sectors are increasingly experimenting with more operational models of cooperation, such as joint fraud operations cells. Modelled on cyber fusion centres, these structures bring together law enforcement, telecom operators, digital platforms, financial institutions and brand protection teams in a shared operational setting. Such hubs enable coordinated analysis and disruption of fraud compounds, mule networks and transnational criminal infrastructure that no single actor could address alone.

Maintain real-time or near-real-time engagement models where appropriate: Given the speed at which fraud campaigns spread, regulatory and enforcement frameworks should enable rapid engagement between authorities and private sector actors. Where appropriate, governments should support mechanisms that allow for real-time or near-real-time sharing of threat intelligence, indicators of compromise and operational insights, enabling faster intervention and harm prevention. Operational cooperation models, including joint taskforces or operations cells, are particularly effective when supported by such real-time engagement capabilities.

Foster trusted environments for intelligence exchange between sectors and authorities: Effective cooperation depends on trust, legal clarity and shared objectives. Governments should foster secure

12 FedPayments Improvement, "About the FraudClassifier Model", accessed October 23, 2025, https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/fraudclassifier-model/

13 FedPayments Improvement, "About the ScamClassifier Model", accessed October 23, 2025, https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/scams/scamclassifier-model/

and trusted environments in which businesses, law enforcement and other relevant authorities can exchange sensitive intelligence in a lawful and responsible manner. Clear rules, safeguards and accountability mechanisms are essential to encourage participation and ensure that information sharing translates into concrete action.

As part of this, policymakers should encourage the availability and use of shared, standardised and privacy-protective tooling to support law enforcement operations. Large technology companies already provide tools such as notice-and-takedown platforms, digital forensic capabilities and structured interfaces for bulk lawful data requests. Standardising such tooling, with transparent governance and strong privacy safeguards, can help speed operational response, reduce administrative friction and enable authorities to act more effectively against organised fraud networks.

Prioritise outcomes: Regulatory approaches should seek to identify and avoid complex or duplicative reporting obligations that divert resources away from frontline prevention and enforcement. Governments should work with industry to design proportionate, risk-based requirements that support meaningful action against fraud, incentivise innovation and allow organisations to focus on protecting users and targeting perpetrators.

Launch (joint) public education campaigns: Empowering individuals with knowledge is a key and effective tool in addressing fraud and most effective if done as a joint effort with other organisations across sectors. Just as raising awareness has been seen as a key and effective public policy tool in addressing threats such as spam and phishing, it remains an essential pillar in the fight against scams and fraud: informed individuals are simply less likely to fall prey to fraudsters.

Beyond traditional awareness campaigns, leading practices increasingly embed consumer protection directly within digital services themselves. This includes “in-flow” safety prompts and contextual warnings that appear during high-risk user journeys as well as intervention messaging triggered when potentially fraudulent or risky activity is detected.

Effective education efforts also benefit from close collaboration with consumer protection bodies and civil society organisations to develop clear, plain-language alerts that resonate with diverse audiences. To ensure inclusivity, educational content should be regionalised, culturally appropriate and accessible to communities with lower levels of digital literacy, helping reduce victimisation while reinforcing trust in digital services.

Key takeaway

Fraud prevention requires sustained, operational cooperation between governments and industry. Structured partnerships, real-time intelligence exchange and trusted collaboration frameworks are essential to effectively reduce harm.

4. Conclusion

Online and ICT-enabled fraud is a shared, transnational threat that undermines trust, inclusion and growth across the global digital economy. Organised criminal groups use technology to exploit fragmentation, speed and scale while the harm is borne by individuals, communities, businesses and governments alike.

Industry is actively investing in prevention, detection and disruption of fraud and scams, but no sector can succeed alone against well-resourced and sophisticated, cross-border criminal networks. Effective responses require interoperable, evidence-based cooperation frameworks that enable swift action against perpetrators.

To effectively combat global fraud and scams, governments should focus on **four priorities**:

1. **Go cross-border by default:** Fraud is transnational – enforcement must be too. Governments should strengthen international legal cooperation, streamline cross-border data access, run joint investigations targeting criminal networks;

2. **Invest in prevention, not just response:** Make scam prevention a national priority with dedicated funding, modernise data and analytical capabilities, build specialised law enforcement skills and enhance fraud intelligence capacity;

3. **Fix legal and regulatory fragmentation:** Governments should clarify laws, enable fraud reporting and intelligence sharing, support responsible AI for fraud detection and provide liability protections for companies acting in good faith. Aim for globally interoperable regulations across consumer safety, cybersecurity, privacy and data protection to reduce legal ambiguity and encourage proactive prevention;

4. **Operationalise public-private cooperation:** Move beyond dialogue to real-time operational collaboration, including joint operations cells, trusted intelligence-sharing platforms and coordinated public education campaigns. Encourage cross-industry and multilateral collaboration to prevent fraud before it happens.

Governments, industry, law enforcement agencies and civil society must work together to strengthen cross-border enforcement, align regulatory approaches and expand operational public-private partnerships. These efforts should aim to disrupt organised criminal groups, protect individuals and businesses and reduce unnecessary regulatory burdens, focusing resources on **the core objective: stopping fraud at its source**.

Additional information

Amnesty International (2025), "Cambodia: Government allows slavery and torture to flourish inside hellish scamming compounds", *Amnesty International*, https://www.amnesty.org/en/latest/news/2025/06/cambodia-government-allows-slavery-torture-flourish-inside-scamming-compounds/.

Council on Foreign Relations (2024), "How Myanmar Became a Global Center for Cyber Scams", *Council on Foreign Relations*, https://www.cfr.org/in-brief/how-myanmar-became-global-center-cyber-scams.

CSIS (2024), "Cyber Scamming Goes Global: Sourcing Forced Labor for Fraud Factories", *Center for Strategic and International Studies*, https://www.csis.org/analysis/cyber-scamming-goes-global-sourcing-forced-labor-fraud-factories.

CSIS (2024), "Cyber Scamming Goes Global: Unveiling Southeast Asia's High-Tech Fraud Factories", *Center for Strategic and International Studies*, https://www.csis.org/analysis/cyber-scamming-goes-global-unveiling-southeast-asias-high-tech-fraud-factories.

Department of Justice (2025), "Multiple India-based call centers and their directors indicted for perpetuating phone scams affecting thousands of Americans", *United States Department of Justice*, https://www.justice.gov/usao-ndga/pr/multiple-india-based-call-centers-and-their-directors-indicted-perpetuating-phone-scams.

GSMA (2025), *Fraud and Scams: Staying Safe in the Mobile World*, GSMA, https://www.gsma.com/solutions-and-impact/connectivity-for-good/public-policy/gsma_resources/fraud-and-scams-staying-safe-in-a-digital-world/.

GSMA (n.d.), *GSMA Use Case Library*, GSMA, https://www.gsma.com/solutions-and-impact/technologies/security/scams/scam-use-case-library/.

Inkstick Media (2024), "How India's Cyber Scam Industry Causes Global Havoc", *Inkstick Media*, https://inkstickmedia.com/how-indias-cyber-scam-industry-causes-global-havoc/.

INTERPOL (2024), "USD 257 million seized in global police crackdown against online scams", *INTERPOL*, https://www.interpol.int/News-and-Events/News/2024/USD-257-million-seized-in-global-police-crackdown-against-online-scams.

INTERPOL (2024), *Interpol Global Financial Fraud Assessment*, INTERPOL, https://www.interpol.int/content/download/21096/file/24COM005563-01%20-%20CAS_Global%20Financial%20Fraud%20Assessment_Public%20version_2024-03_EN_v3.pdf.

INTERPOL (2025), "INTERPOL releases new information on globalization of scam centres", *INTERPOL*, https://www.interpol.int/News-and-Events/News/2025/INTERPOL-releases-new-information-on-globalization-of-scam-centres.

Tech Policy Press (2024), "How Technology and Regulatory Gaps Fuel Scam Compounds", *Tech Policy Press*, https://www.techpolicy.press/how-technology-and-regulatory-gaps-fuel-scam-compounds/.

TRT World (2024), "Exclusive: How Indian scammers built a multi-billion-dollar global fraud empire", *TRT World*, https://www.trtworld.com/article/23e1fe1c3220.

United Nations Office on Drugs and Crime (2023), *Casinos, cyber fraud, and trafficking in persons for forced criminality in Southeast Asia: Policy report*, United Nations Office on Drugs and Crime, https://www.unodc.org/roseap/uploads/documents/Publications/2023/TiP_for_FC_Policy_Report.pdf.

United Nations Office on Drugs and Crime (2024), "Crushing scam farms, Southeast Asia's 'criminal service providers', *United Nations Office on Drugs and Crime*, https://www.unodc.org/unodc/frontpage/2024/July/crushing-scam-farms--southeast-asias-criminal-service-providers.html.

United Nations Office on Drugs and Crime (2025), *Southeast Asia and the Pacific Organized Crime Threat Alert*, United Nations Office on Drugs and Crime, https://www.unodc.org/roseap/uploads/documents/Publications/2025/UNODC_Alert_Strategic_infiltration_of_vulnerable_jurisdictions_through_criminal_foreign_direct_investments.pdf.

YouTube (2022), *India's Thriving Scam Industry: Before You Call Tech Support | Undercover Asia*, https://www.youtube.com/watch?v=7CZReZ24-to.

About the International Chamber of Commerce

The International Chamber of Commerce (ICC) is the institutional representative of more than 45 million companies in over 170 countries. ICC's core mission is to make business work for everyone, every day, everywhere. Through a unique mix of advocacy, solutions and standard setting, we promote international trade, responsible business conduct and a global approach to regulation, in addition to providing market-leading dispute resolution services. Our members include many of the world's leading companies, SMEs, business associations and local chambers of commerce.

33-43 avenue du Président Wilson, 75116 Paris, France
T +33 (0)1 49 53 28 28 E icc@iccwbo.org
www.iccwbo.org @iccwbo