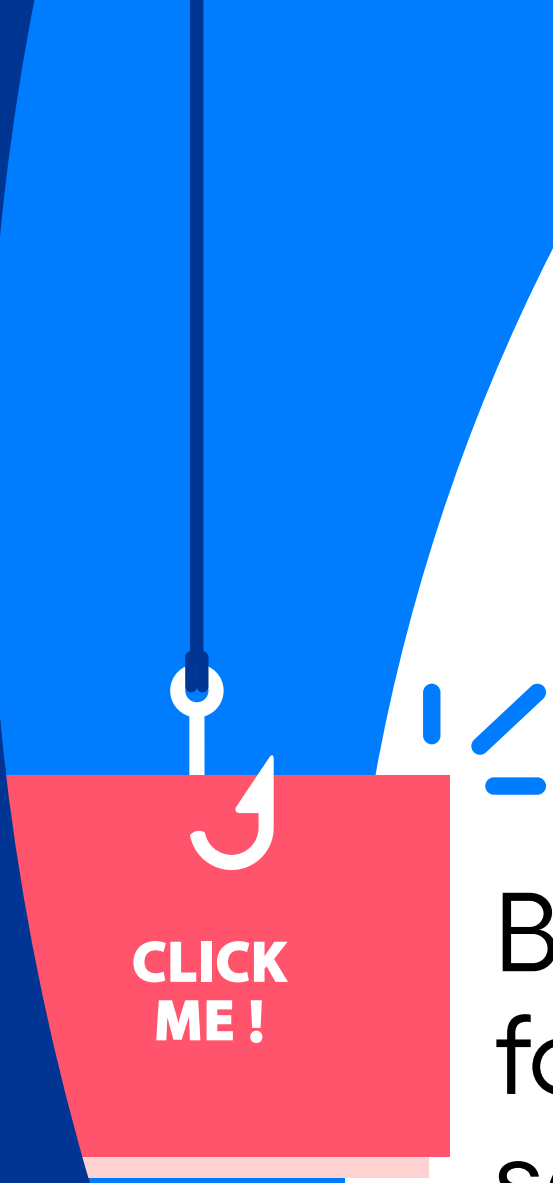

Best practices for combating scams in advertising

ICC GASA

Table of contents

I. Introduction and context

The challenge of scam advertising

Recent research by the Global Anti-Scam Alliance (GASA) estimates that scams cost individuals and businesses worldwide an estimated $442 billion annually.[1]

Scams are harmful to consumers and legitimate businesses. Online scams are a growing global problem, affecting people of all ages and backgrounds.[2] The perpetration of scams via digital infrastructure, including digital advertising, undermines individual users' trust in the digital and advertising ecosystems, imposes significant economic costs, and harms individuals and communities worldwide.

Scammers are constantly evolving their tactics and taking advantage of new technologies and social trends. The convergence of targeted advertising driven by artificial intelligence (AI), automated payment systems, anonymisation technologies, and global networks has created a complex criminal ecosystem that transcends borders. Fraudsters disguise illicit content as legitimate online ads or lure victims through off-platform links, while payments are processed through overseas servers – making tracing and enforcement an ongoing challenge.

Scam risks in advertising should not be understood narrowly. Increasingly, fraudulent activity emerges through a broader cross-platform ecosystem in which deceptive paid content, influencer-style promotion, impersonation, messaging applications and financial or crypto-related inducements can interact in the same scam journey. In many cases, advertising is not the end-point of the harm but the entry point into a wider manipulation chain that may rapidly move users to off-platform environments where enforcement becomes more difficult.

The scale of the challenge is further shaped by the volume and diversity of advertisers operating online. The vast majority of these – small businesses, sole traders and new market entrants – are entirely legitimate, and ensuring they can access digital advertising with minimal friction is an important objective in its own right. However, this population also presents verification challenges that scammers seek to exploit, deliberately targeting the points in the ecosystem where oversight is hardest to apply systematically and at scale.

The role of the International Chamber of Commerce

Through its Global Marketing and Advertising Commission, ICC has a long-standing commitment to promoting high standards of ethics in marketing and advertising, most notably through the ICC Advertising and Marketing Communications Code (the ICC Code)[3], a global framework for responsible marketing communications. By promoting self-regulation in the business sector in accordance with globally recognised high ethical and legal standards, consumers can be confident that businesses

---

1 GASA, Global State of Scams 2025

2 Australia: More than 108,000 scam reports in the first half of 2025, with total losses amounting to AU$173.8 million, up 26% from the same period in 2024 (ASC, National Anti-Scam Centre calls for continued action this Scams Awareness Week as scam losses trend up at $174M, August 25, 2025).
Korea: Losses from voice-phishing crimes between January and August 2025 reached KRW 885.6 billion — surpassing the total losses recorded in 2024 (KRW 854.5 billion) (***Maeil Business Newspaper***. Phone Scams Now Cost Over 1 Trillion Won Annually—Voice Phishing Has Become a National Disaster, September 21, 2025); 273,000 fraudulent accounts detected linked to illegal financial advertising and investment solicitations between August 2024 and June 2025. (***The Korea Economic Daily***. FSS, Kakao, and Google Block 270,000 Illegal Ads… Full Expansion of Co-Regulation, August 5, 2025)
UK: The Financial Conduct Authority (FCA) withdrew or amended 19,000 inappropriate or illegal financial advertisements in 2024 — nearly double the number from the previous year (FCA, FCA steps up action against misleading financial adverts, July 2, 2025).

3 ICC, Advertising and Marketing Communications Code

abiding by the ICC Code and related ICC guidance can be relied upon to provide advertising that is legal, decent, honest and truthful, fostering a robust marketplace that both enhances creativity and preserves consumer trust.

ICC's approach to scam prevention recognises that fraudulent advertising often exploits consumer trust through impersonation and the misuse of well-known brand identities, copyrighted content or other protected assets. In practice, reporting based on intellectual property (IP), brand verification and notice-and-takedown mechanisms therefore form an important part of the broader enforcement landscape alongside platform-level measures. While this paper focuses on advertising-specific interventions, these issues are addressed through ICC's wider work on intellectual property, cybersecurity and its policy framework on preventing online and fraud enabled by information and communications technologies (ICT).

The role of the Global Anti Scams Alliance

GASA is a global non-profit coalition committed to protecting consumers worldwide from scams through cross-sector collaboration, research, and the development of actionable best practices. By bringing together policy makers, law enforcement, consumer authorities, and the private sector, GASA facilitates the sharing of critical insights and knowledge to disrupt scam ecosystems. Through its commitment to enabling hands-on tools and fostering a global network of expertise, GASA aims to promote a safer digital environment, empowering stakeholders to work collectively to preserve user trust and security across the online landscape.

The purpose of this guidance

The primary purpose of this paper is to establish a clear and effective strategic direction for the industry to address the challenges posed by fraudulent paid advertising. By outlining these objectives and sharing best practice, this document aims to provide insight into the steps taken by responsible actors, the effective practices that can be taken to support consumers and to prevent bad actors from misusing the advertising ecosystem, and promote their adoption across relevant platforms and internationally. It also seeks to articulate the value of collaboration amongst all interested parties, from regulators and law enforcement to the private sector and relevant technical community and civil society actors in order to most effectively tackle this issue.

This guidance is intended to complement, and not replace, applicable legal and regulatory obligations. Where appropriate, it may also help identify best practices that go further than minimum legal requirements in areas where stronger or more effective preventive action is needed.

This paper is also intended to serve as a sector reference framework that can help reinforce trust, responsibility and coherence across the advertising and marketing ecosystem.

II. Key principles for combating scam advertising

Prioritising user trust and safety

The ad-supported internet relies fundamentally on maintaining high standards of user trust and safety, which are undermined by the rise of online scams. To combat this, there is an urgent need for continuous investment in developing and improving robust policies, products, and processes designed specifically to protect users from fraudulent activity.

Trust should be regarded not merely as a consumer protection outcome, but as a core condition for the long-term legitimacy and effectiveness of the digital advertising ecosystem. A healthy ad-supported internet depends on the ability of users, advertisers and intermediaries to rely on systems that are transparent, responsible and proportionate. Measures against scam advertising should therefore support both user safety and the broader resilience of legitimate digital commerce.

Multi-layered, responsive approach to ads safety

No single method offers a solution to the complexity of tackling scams globally. Methods need to be regularly adapted, particularly in order to tackle the risks arising from the adoption of generative AI and deepfake technologies by scammers. Consequently multi-layered, responsive frameworks are vital. These should incorporate verification at relevant points in the course of interactions with an advertiser and in response to information that becomes available to a platform and be complemented by additional controls. They should include regular analysis of advertisers' behavioural patterns and transaction histories in order to ensure that assessments of risk levels remain up to date and that proportionate measures are applied in response to changes to this level.

The necessity of a risk-based and proportionate approach

The same advertising systems used by scammers to reach victims are those used by millions of legitimate businesses worldwide to reach users. A balance must be struck between ensuring that legitimate businesses have easy access to the services that they need and implementing safety controls which inhibit bad actors (where the friction of verification and account security settings can help mitigate the harm they seek to cause).

In order to achieve this balance, friction and account security measures imposed on advertisers must be proportionate to the risk they present to the ecosystem. Such measures may be of increasing intensity according to an advertiser's risk level, enabling sound risk management while minimising burden on legitimate businesses operating in low-risk areas. In addition, the nature of the restriction may vary, whether by restrictions on exposure, functionality or payment options, depending on the signals available. With this approach, disproportionate data collection for low-stakes interactions is avoided and resources can be focused where risk is highest, amplifying the value of this risk-based approach.

Human oversight and accountability

While automated systems play an essential role in detecting, assessing and mitigating scam-related risks, responsibility for anti-scam governance should not be delegated to technology alone. Scam prevention mechanisms should remain subject to meaningful human oversight, particularly in higher-risk situations involving impersonation, financial services, coordinated deception or other forms of serious consumer harm.

Such oversight helps ensure that decisions with significant consequences for advertisers, users or market access remain explainable, reviewable and proportionate. It also helps preserve confidence in anti-scam systems by reducing the risk of outcomes that may be insufficiently sensitive to context, evolving tactics or legitimate commercial activity.

Industry participants should therefore ensure that automated verification, detection and enforcement tools are supported by clear escalation paths, appropriate review mechanisms and internal accountability structures.

This is a rapidly evolving space; as large language models (LLMs) and agentic AI capabilities mature, the technical ability to adjudicate complex risk and business operations will increase. Consequently, the nature of "meaningful oversight" may shift from manual intervention to AI-governed accountability systems that can scale to match the volume of digital advertising.

Collective defence

No one participant or type of participant can prevent scams alone. Collaboration across the public and private sector is essential to mount an effective global response to bad actors. In particular information-sharing networks which involve regulators, law-enforcement, platforms, financial institutions, telecom providers and domain registrars and industries are emerging as a promising model for public-private cooperation. These should provide opportunities for information sharing both with respect to trends and specific signals which identify bad actors and support ongoing, iterative approaches to the combating of scams. Legal frameworks which support such information sharing, provide paths to law enforcement and which allow for flexibility in the approach to tackling scams will contribute to the collective defence.

Consideration should also be given to established defence and information exchange mechanisms, such as those that exist for IP protection, in order to benefit from existing and ongoing work in these areas.

Effective collective defence requires coordinated action across the full advertising ecosystem, including platforms, advertisers, agencies, self-regulatory organisations, financial-sector stakeholders, trusted flaggers, technical intermediaries, public authorities, such as government departments, regulators and law-enforcement and consumer-protection bodies. Scam advertising often exploits the gaps between these actors; stronger coordination is therefore needed not only to detect bad actors, but also to reduce fragmentation in response and accelerate intervention across the scam pathway.

III. Best practices for platforms, agencies and others to combat scams

Those entities who have direct relationships with advertisers, in particular platforms and agencies, should adopt and continually evolve best practices to mitigate risk and protect consumers. The below sets out current best practice as it relates to key principles of effective scam-fighting by advertising platforms and agencies. At their core these rely on an assessment of the risk level of specific advertisers, their content and behaviour and provide a strong structural foundation to anti-scam efforts.

A. Risk-mediated progressive verification systems

Platforms

Initial assessments

Strong protection against bad actors can be put in place from the outset of the relationship between an ad platform and advertisers. A tiered verification system implemented at this stage acts as an intelligent "front door" security check for the advertising ecosystem, stopping malicious actors at the source, before any harmful ads can reach consumers. A flexible approach allowing for standard verification for advertisers not assessed as high risk ensures that legitimate businesses – especially small and medium-sized businesses – can operate without undue friction. Steps 1, 2A, 2B and 3 below reflect best practice in assessing and responding to the risk posed by new advertisers. They provide a framework within which additional tiers of checks can be implemented as required.

1

Step 1: Trust assessments on all advertisers

Platforms should apply proportionate systems and processes to carry out an initial trust assessment for every advertiser soon after account creation as part of the advertiser's onboarding process (or at the point where conversion of a user account to a paid advertiser account takes place). This initial assessment, conducted before advertising content is displayed, should be based on reasonably available and proportionate behavioural and relational signals to determine an initial risk classification and should include measures to identify previously terminated or suspended advertisers. Platforms should keep their criteria under review to ensure that they remain relevant.

2a

Step 2a: Advertisers assessed as high-risk at trust assessment

This measure applies to **advertisers who, following a trust assessment, are identified as high risk.**

For these advertisers, the platform should:

a. require the advertiser to complete enhanced verification, and
b. prevent the advertiser from serving advertisements on the platform's service until the platform is satisfied (acting reasonably), following the successful completion of enhanced verification that the advertiser does not pose a significant risk.

Enhanced verification should entail a high-assurance verification process. By necessity, this will evolve over time but is likely to include verification:

- of the identity of the individual completing the process using methods that provide a high level of assurance;
- that the advertiser is affiliated with the business on behalf of whom it purports to be advertising; and
- of basic information about the advertiser's business operations.

It is likely that within the high-risk cohort, there is further scope to tailor verification methods to the nature and severity of the risk. While IAL3 (NIST 800-63A) may be necessary in certain narrow, high-risk scenarios, it may also present significant friction for many legitimate commercial entities. Consequently, the development of additional intermediate standards for digital commerce could help support this balanced approach.

2b

Step 2b: Standard advertiser verification for all other advertisers

For all advertisers **not classified into the high-risk cohort** at the trust assessment stage:

For these advertisers, the platform may permit the advertiser to serve ads after the initial trust assessment is complete and should:

a. require the advertiser to complete advertiser verification within a reasonable time period after onboarding; and
b. suspend the advertiser's ability to serve any advertisements where such advertiser has failed to successfully complete advertiser verification.

Such a baseline verification process required for all advertisers not classified into the high-risk cohort may verify:

- the legal identity of the individual completing the process and
- the legal name of the organisation on whose behalf they are advertising.

This process may be implemented using automated methods to help facilitate access to digital advertising and enable any relevant transparency requirements to be met. In this context, digital IDs may be a useful tool for standardisation and provide a low-friction high security method of establishing this level of assurance.

3

Step 3: Additional requirements for advertisers of financial services

In addition to the verification requirements above, for advertisers of financial products or services that platforms have observed to be vulnerable to abuse in a relevant jurisdiction, platforms should take steps to confirm that the advertiser is authorised by the relevant regulator and appears on the relevant financial services register (unless that advertiser is legally permitted to place financial product or services paid-for advertisements without further authorisation by that regulator).

The continued improvement of national registries is vital to the ability of platforms to implement these controls effectively. Registers should be kept up-to-date, machine-readable via CSV or API access and accessible to platforms at scale, and should include data fields covering all domains

from which a licensed provider is permitted to operate and active corporate contact details. Critically, registers should be refreshed frequently enough to reflect changes in authorisation status in near real-time, ensuring that revoked or lapsed licences are promptly reflected and cannot be exploited during the interval between revocation and register update. Regulators are strongly encouraged to share best practice on registry standards and to ensure that their registers meet the minimum requirements set out in Section IV of this paper.

This measure establishes an additional check in a high-stakes sector where consumer harm can be particularly egregious. Sector-specific authorisation confirming the advertiser has the credentials to offer a particular service provides an additional layer of friction on top of identity verification, which applies to all advertisers.

Additional requirements for other verticals

In addition to the requirements for financial services above, platforms should consider enhanced verification requirements for other sectors where there is demonstrable evidence of persistent or systemic fraudulent advertising and where verification presents an effective means of determining the status of an advertiser. Regulated sectors, including gambling and pharmaceuticals, warrant particular attention in this regard. When assessing the implementation of such additional checks, the quality of relevant data and robustness of the regulatory regime associated with it are material considerations.

Continuous risk assessment and re-classification

A platform's trust assessment of an advertiser should be a continuous process, not limited to a one-time check at onboarding, and should use ongoing monitoring based on reasonably available and proportionate behavioural and relational signals. Platforms should also draw on external authoritative signals, including information shared by regulators, law enforcement, industry bodies and other platforms, where reasonably available and reliable, and subject to applicable legal constraints, to supplement their internal monitoring capabilities and ensure that risk assessments reflect the broadest possible intelligence base.

Where such signals indicate that an advertiser who was not initially deemed high-risk may now pose a high risk of serving fraudulent advertisements, the platform should require that advertiser complete enhanced verification and should suspend ad delivery until that verification has been successfully completed.

These requirements are crucial for combating sophisticated adversarial actors who appear legitimate and pass initial checks before engaging in fraudulent activity. Continuous assessment ensures that trust is not a one-time grant but an ongoing status that must be maintained, allowing platforms to adapt dynamically to advertisers whose risk profile changes over time.

Platforms should also consider providing regular transparency to an appropriate audience about the evolution of their advertiser verification and anti-scam controls, including, where appropriate, updates on policy development, verification approaches, identified abuse trends and improvements introduced in response. Such transparency, provided it does not require disclosure that would undermine the effectiveness of anti-fraud systems, can help strengthen accountability, support industry learning and encourage continuous improvement across the ecosystem.

Proportionate limitations on high-risk advertising activities

In addition to the above, when an advertiser, who has not been assessed as high-risk, engages in specific advertising activities that a platform has observed to be associated with an emerging scam trend, additional measures may be appropriate. These activities may include attempting to serve paid-for advertisements in risk-prone topic areas. In these circumstances, and particularly if the advertiser does not have a longstanding record of safe advertising, the platform should apply proportionate measures to mitigate potential harm. Such measures may include limiting the visibility of the advertiser's paid-for advertisements in that specific risk-prone topic area or content category until after the advertiser establishes a sufficient record of safe advertising.

This measure allows platforms to innovate and develop surgical tools to manage emerging threats without resorting to broad, commercially disruptive policy changes. Advertisers should progressively earn the privilege of accessing risk-prone topic areas or sensitive product features after establishing a track record of safe advertising.

Agencies

Agencies are well placed to interrogate the identity of their customers and determine their credibility. Similarly to platforms, agencies can introduce strong protections against bad actors from the outset of their relationship and the implementation of Know Your Customer (KYC) protocols helps to ensure that they are introducing trusted advertisers to the ecosystem. A flexible approach, allowing for risk assessments in order to determine where greater vigilance is required should be adopted.

Agencies should have procedures in place to facilitate the review of new information about advertisers and to effect offboarding where fraudulent advertisers are identified.

B. Complementary safety-by-design features

While verification systems act as an essential "front door", efforts to detect and interrupt scammers should not end there because scammers will seek to bypass these controls and may hijack legitimate advertiser (or other user) accounts. The incorporation and use of "safety-by-design" features by platforms, agencies and advertisers ensures that the advertising ecosystem remains resilient even after an advertiser has been onboarded.

1. Robust account protection mechanisms

Account takeover is also a known vector for scam advertising. Scammers use phished credentials or session hijacking to serve malicious ads from legitimate accounts, exploiting the account holder's established trust and payment history.

- **Multi-factor authentication (MFA):** As a safeguard against account takeover, platforms should consider requiring multi-factor authentication (MFA) for advertiser accounts. To be effective, platforms should promote phishing-resistant MFA and avoid sole reliance on weaker forms such as SMS-based one-time passwords, which are vulnerable to SIM swapping and interception.
- **Session integrity and adaptive challenges:** Platforms should implement features that detect anomalous access patterns, such as logins from geographically distant locations in a short timeframe ("impossible travel") or suspicious device fingerprints. These should trigger re-authentication or temporary account locks when high-risk changes are made, such as adding a new payment method or significantly increasing daily spend.

- **Least privilege access controls:** Agencies and large advertisers should utilise granular permission settings based on the principle of least privilege. Access to sensitive functions, such as modifying destination URLs or exporting customer lists, should be restricted to specific authorised roles to minimise the potential impact or "blast radius" of a single compromised credential.
- **Corporate email domain enforcement:** For enterprise or agency accounts, platforms should provide the capability to restrict account access exclusively to specific, verified corporate email domains. This prevents "shadow" access by unauthorised personal accounts and ensures that when an employee leaves an organisation, their access can be revoked centrally via the corporate directory.

2. Addressing common advertiser safety flaws

Scammers frequently exploit common technical and procedural oversights by legitimate businesses. Awareness and proactive mitigation of these flaws are vital for maintaining a clean ecosystem.

- **Destination URL monitoring:** A common tactic involves "cloaking", where a legitimate URL is shown during the ad review process but is swapped for a scam site once the ad is live. Platforms should implement automated scanning of landing pages at regular intervals throughout the lifecycle of the campaign to detect such unauthorised changes.
- **API security:** For advertisers and agencies using automated tools, securing API keys is critical. Compromised keys can allow scammers to launch scam ads programmatically. These keys should be regularly rotated and restricted to specific IP ranges.

3. Intelligence-led identification and prevention of recurring scam patterns

Platforms should implement proactive systems designed to identify and mitigate recurring scam patterns, including the use of similarity detection tools capable of flagging substantially identical ads associated with known fraudulent activity. They should continuously update their methodologies in response to new threat vectors. Effective record keeping and retention of verification information may support more effective detection.

Platforms should act on relevant intelligence from trusted flaggers and industry partners to block associated fraudulent advertising activity and prevent the iterative reintroduction of harmful ads.

4. Block lists and collaborative enhancement

Platforms should maintain and actively manage block lists of known fraudulent advertisers, domains, payment identifiers and other signals associated with scam activity. To be effective, block lists must be treated as living tools that require continuous updating, especially given the ease of creating new domains and URLs to host fraudulent and scam content.

5. Proactive education and communication

Communication and public education represent another way in which participants across the ecosystem can contribute to scam prevention. Many can speak publicly with authority about the risks posed by scams and how individuals and groups can protect themselves. When doing so, it will be vital to consider existing best practice that promotes the use of trauma-informed and accessible language and the use of active inoculation and engagement campaigns alongside passive awareness campaigns. Within the advertising community there are experts who can contribute the creativity and know-how to amplify

messages and drive engagement. Participation in awareness campaigns is strongly encouraged, although such interventions require rigorous monitoring and evaluation, and lessons learned should be widely shared across the ecosystem.

More specifically, all participants should consider relevant touchpoints with users that enable them to provide information and alerts about the risks posed by scammers. For example, platforms and agencies should provide safety health checks or dashboards that alert advertisers to security gaps, as well as:

- **Point of risk notifications:** Alerts triggered at the moment a user is about to take a potentially risky action.
- **Security notifications:** Real-time alerts for login attempts from new devices or changes to critical account settings.
- **Best practice guidance:** Clear, actionable messaging within the user interface regarding the risks of disabling security features or using weak authentication methods.

C. Enhancing transparency and user control

Transparency

Advertiser transparency is a foundational element of consumer protection in the digital advertising ecosystem. Platforms should require advertisers to disclose their official name and country of legal establishment and should make this information available to users in real-time through a clearly accessible disclosure mechanism such as an "About this Ad" feature. This provides users with the means to make informed assessments about the provenance of advertising they encounter and gives regulators and law enforcement meaningful visibility into participants in the advertising ecosystem.

The transparency measures described above are most readily achievable where a direct relationship exists between the platform and the advertiser. In the open programmatic ecosystem, however, advertiser identity can become separated from the campaign as it passes through multiple intermediaries – demand-side platforms, supply-side platforms, ad exchanges and resellers – before it is published. This creates a visibility gap in which no single participant in the chain has complete oversight of the advertiser's identity or the verification standards applied to them.

A particular concern is the practice of aggregating lower-tier demand-side platform campaigns and reselling them to more premium demand-side platforms. This can effectively allow scam advertisers to access premium publisher environments and more credible ad placements without being subject to the verification standards those environments would apply to direct advertiser relationships. It also creates a re-entry risk: advertisers removed from one part of the ecosystem can potentially re-enter through a different point in the reselling chain.

To address this, platforms, publishers and intermediaries operating in the programmatic ecosystem are encouraged to adopt the IAB Tech Lab supply chain transparency specifications, including sellers.json, buyers.json, ads.txt and the SupplyChain object. These provide the foundational infrastructure for making reselling relationships more transparent and auditable.

Reporting

Reporting channels which allow for identification of suspicious or fraudulent ads to platforms are vital to ensure comprehensive defence against scams and enable the detection of new trends and loopholes. Such reporting channels should:

- provide for real-time reporting with easy identification of the reported asset;
- differentiate treatment depending on the status of the reporter, for example by providing priority flagging routes for trusted reporters such as specialist regulators, law-enforcement and self-regulatory bodies; and
- enable the platform to gather all of the information they need in order to identify the content being reported while being quick and easy for a user to submit and allow for timely action by the platform.

National and international bodies engaged in the detection of scams should familiarise themselves with reporting mechanisms and engage with platforms to ensure effective use of these tools.

D. Participating in scam lead and intelligence sharing

Timely information exchange is central to combating online scams and establishing a collective defence against scam advertising. To this end, use of real-time signal exchange mechanisms is strongly encouraged. Such systems should be guided by clearly defined rules on data standardisation, information verification and update procedures, and privacy and security safeguards.

Given the speed at which scam campaigns can spread across services and jurisdictions, rapid signal sharing mechanisms are essential. Where credible indicators of fraud are identified, platforms and relevant intermediaries should be able to act swiftly to review, suspend or block suspicious advertisements, accounts or related assets, while ensuring that such measures remain proportionate and supported by appropriate safeguards.

Where practical, intelligence-sharing mechanisms should be designed to capture the full scam pathway rather than isolated ad assets alone. In practice, this means enabling the reporting of linked domains, advertiser identities, cloned brand signals, payment-related indicators and off-platform destinations, including messaging or social channels where relevant. A more joined-up approach to signal exchange can materially improve the detection of repeat offenders, coordinated campaigns and scam migration across services.

Example: The Global Signal Exchange[4] (GSE), an independent non-profit based in the UK, which has been co-founded by Oxford Information Labs, Google and the Global Anti-Scam Alliance, enables platforms, intermediaries, and security partners, including cybersecurity firms and law enforcement agencies, to share threat intelligence in real time about fraudulent activity and scam campaigns to facilitate cross-industry disruption and promote collective defence. The potential of such mechanisms is demonstrated by a pilot malvertising project led by the Advertising Association in the UK involving the GSE, Google and Amazon, which has tested how shared threat signals can be operationalised across major platforms to identify and share malicious URLs.[5]

4 https://www.globalsignalexchange.org/

5 https://www.gov.uk/government/publications/online-advertising-taskforce-progress-report-2025/online-advertising-taskforce-progress-report-2025#:~:text=support%20as%20necessary.-,Information%20Sharing,-Objective

IV. Collaboration to strengthen the collective defence

Effective scam prevention requires stronger operational coordination and information-sharing between advertisers, agencies, digital platforms and other relevant actors across the advertising value chain.

The ability of those engaged in the work of protecting their services and users from bad actors requires both support of local regulatory agencies and legislative frameworks that enable them to enhance protections without increasing their potential exposure to liability for the actions of bad actors.

The nature of such support will take differing forms over time and should be kept under continuous review. A number of proposals are set out below.

Consistency and data integrity in national registries

Accurate, accessible and up-to-date national licensing registers are a critical operational precondition for scaling advertiser verification in high-risk sectors globally. Without reliable registry data, platforms cannot effectively confirm whether an advertiser is genuinely authorised to offer the services they claim to provide, undermining the verification framework set out in Section III.

The following standards are strongly recommended for national licensing registers:

- Registry data should be accurate, comprehensive and maintained to a high standard of data integrity.
- Registers should be refreshed frequently enough to reflect changes in authorisation status in near real-time, ensuring that revoked or lapsed licences are promptly reflected and cannot be exploited during the interval between revocation and register update.
- Data should be machine-readable and directly accessible to platforms, for example via API or CSV, to enable scalable queries without manual intervention.
- Registers should include, at minimum, all domains from which a licensed provider is permitted to operate and active corporate contact details. This is vital to mitigate the risk presented by registry scraping because it enables authentication by the platform.
- Greater interoperability between national registers, and where relevant transnational registers, would materially strengthen cross-border verification and reduce the risk of jurisdiction shopping by fraudulent advertisers.

For higher-risk sectors, the quality, accessibility and interoperability of official registries are not merely administrative concerns – they are operational safeguards on which effective scam prevention depends.

This applies across all licensed and regulated sectors, including financial services, gambling and healthcare services, where scammers frequently impersonate authorised firms, regulated professionals or well-known market actors.

Effective collaboration with law enforcement and support for international interventions

Scam advertising is a practice which crosses multiple international borders. Perpetration and harm are rarely confined to a single jurisdiction. Consequently, law enforcement and government agencies must be engaged to disrupt criminal enterprises (e.g., scam compounds) at their root and this requires international efforts to share information and encourage intervention, as covered in detail in a 2026 ICC issue brief.[6]

Promoting safe harbours

Governments play an important role in creating the legal conditions necessary for effective scam prevention. Two areas are particularly important: liability protections for proactive enforcement action, and legal frameworks that enable platforms and other actors to share scam-related intelligence without undue legal risk.

On liability, a service should not become liable for information it hosts simply because it has taken voluntary, good faith action to detect and remove fraudulent content. Without such protection, platforms face a perverse incentive to do less rather than more — proactive enforcement efforts that are imperfect may expose them to greater liability than taking no action at all. Good Samaritan liability protections address this by shielding platforms and intermediaries from liability arising from their proactive efforts to identify and remove harmful content, even where those efforts are not always successful. The EU Digital Services Act and section 230 of the US Communications Decency Act are examples of how such protections can be embedded in a broader regulatory framework.

On information sharing, platforms and intermediaries that share scam-related signals and threat intelligence with other industry participants, regulators or law enforcement should have appropriate legal certainty that doing so in good faith does not expose them to liability under data protection, competition or other legal frameworks. The absence of such certainty is a material obstacle to the kind of collective defence the paper advocates. Governments should consider whether existing legal frameworks adequately support good faith information sharing for scam prevention purposes, and introduce targeted safe harbour provisions where they do not.

6 ICC, Preventing online and ICT-enabled fraud, 2026

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.

About the Global Anti Scams Alliance

The Global Anti-Scam Alliance (GASA) is an international organization that brings together public and private sector stakeholders to better understand, prevent, and respond to scams. With over 100 member organizations worldwide, including leading financial institutions, technology companies, and government bodies, GASA serves as a collaborative platform for coordinated action against scams.

Scams have become a widespread global problem, affecting individuals, businesses, and economies across borders. GASA exists to support coordinated, cross-sector efforts that reduce consumer harm and strengthen collective responses to scam activity.