Keoghs
a Davies business

Keoghs LLP response to Ofcom's consultation on the Fraudulent Advertising Codes of Practice

October 2026

Introduction

Keoghs welcomes the opportunity to respond to Ofcom's consultation on the proposed Fraudulent Advertising Codes of Practice.

Keoghs is a leading UK law firm specialising in the defence of insurance claims. We act for eight of the ten largest UK general insurers and provide an end-to-end claims service to insurers, public sector bodies and self-insured organisations. Our Counter-Fraud team works closely with insurers to identify, investigate and disrupt fraud across motor, casualty, property and other insurance lines.

Our response is informed by our practical experience of insurance fraud, discussions with insurer clients, and our wider engagement with government, parliamentarians, law enforcement and the insurance industry on fraud prevention.

Keoghs supports the broad direction of Ofcom's proposals. Effective advertiser verification, account integrity controls, fraud indicator assessments, moderation systems and governance requirements are all necessary if the duties in the Online Safety Act 2023 are to deliver meaningful consumer protection.

Our principal concern is the speed with which the regime is being implemented. The Online Safety Act received Royal Assent in 2023, but Ofcom does not currently expect to publish its final Statement until mid-2027 at the latest. During this period, fraudulent advertisements continue to expose consumers to financial, emotional and wider harm.

Fraud is an adaptive and highly organised activity. Fraudsters can create new advertisements, accounts, domains and identities considerably faster than reports can be investigated and individual content removed. Insurers frequently describe the present position as a game of 'whack-a-mole': once one advertisement or account is removed, the same actor, brand, contact route or underlying infrastructure reappears through another account.

The Codes should therefore be finalised and implemented as quickly as possible. They must prioritise prevention, cross-account disruption and repeat-offender detection, rather than relying principally on the removal of individual advertisements after they have already reached consumers.

Volume 1: Context

Online advertising ecosystem

Is there any information or evidence you hold that could enhance our understanding of the online advertising ecosystem?

Keoghs agrees that the complexity and opacity of online advertising pathways can make it more difficult to identify responsibility for fraudulent advertisements. However, this complexity should not reduce the responsibility of the provider on whose service the advertisement is ultimately displayed.

Consumers cannot reasonably be expected to understand whether an advertisement has been placed through an owned-and-operated system, an advertising intermediary, an affiliate network, a direct arrangement, or an open-display supply chain. From the consumer's perspective, the advertisement appears on the provider's service and may benefit from the apparent credibility of that service.

Providers also retain important forms of control. They determine which intermediaries they work with, the terms on which advertising is carried, the data and technical standards required of participants, and whether particular advertisers, domains or categories of advertisement may access their inventory.

Ofcom should therefore avoid creating a framework in which fragmented advertising pathways also fragment accountability. The provider displaying the advertisement should retain responsibility for ensuring that suitable controls apply throughout any pathway it chooses to use.

Our experience also suggests that the ecosystem should be understood as extending beyond the advertisement itself. A fraudulent campaign may involve:

- an advertising account;
- one or more related personal or business accounts;
- an intermediary or affiliate;
- a payment method;
- a telephone number or messaging account;
- a website, domain or landing page;
- copied insurance branding or documentation;
- an impersonated insurer, broker or claims function; and
- further communications with the consumer outside the original service.

Effective intervention must therefore be campaign-based and network-based. Removing an individual advertisement will rarely be sufficient if the associated accounts, domains, payment arrangements and linked infrastructure remain operational.

Particular consideration should be given to affiliate networks and lead-generation arrangements. The immediate advertiser may present itself as an introducer, marketing business or claims assistance service, while the consumer may reasonably believe they are dealing directly with their insurer, broker or another regulated organisation. Responsibility and beneficial ownership may be obscured through layers of affiliates and associated businesses.

Causes and impacts of fraudulent advertising

Do you have any comments on Ofcom's assessment of the causes and impacts of fraudulent advertising? Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.

Keoghs broadly agrees with Ofcom's assessment. It appropriately recognises the scale of fraud, the use of paid advertising to reach consumers at speed, the role of impersonation and AI, the effect on consumer trust, and the significant financial and psychological impacts on victims.

We consider that the analysis could give greater emphasis to the following matters.

Insurance-specific fraud

Fraudulent insurance advertising should be treated as a significant category in its own right. Two particularly relevant manifestations are ghost broking and paid ad spoofing.

Ghost brokers commonly advertise purportedly discounted motor insurance through social media. They may forge insurance documents, manipulate proposal information to secure an artificially low premium, or arrange a genuine policy and subsequently cancel it. A consumer may not discover that they are uninsured until they are stopped by the police or attempt to make a claim.

The effects extend beyond the initial payment to the fraudster. A victim may:

- drive without valid insurance;
- face seizure of their vehicle;
- be unable to recover losses following an accident;
- incur the cost of replacement insurance;
- face criminal or regulatory consequences; and
- cause losses that ultimately fall on insurers or compensation arrangements for uninsured driving.

Paid ad spoofing commonly occurs when a consumer searches online for an insurer or claims telephone number following an accident. Fraudsters or misleading claims businesses purchase prominent search advertising which imitates the insurer's name, branding or claims service. A consumer may then be diverted into a claims, credit hire, recovery, storage, repair or personal injury arrangement without appreciating that they are not dealing with their insurer.

This is particularly harmful because the consumer may be at the roadside, distressed and looking for urgent assistance. The advertisement exploits both the insurer's brand and the consumer's situational vulnerability. Potential consequences include inflated credit hire, recovery and storage charges, unnecessary repair or rehabilitation arrangements, the collection and onward use of personal data, and funding arrangements under which significant deductions may be made from compensation.

In addition, where misleading advertising diverts consumers away from what they reasonably believe to be their insurer's claims service, there may be reduced opportunity to identify fraud concerns, support vulnerable customers and intervene before avoidable costs are incurred. This can contribute to increased claims inflation through unnecessary recovery, storage, repair and credit hire arrangements that would not otherwise have arisen.

Secondary and cumulative loss

The assessment should more expressly recognise that the loss caused by fraudulent advertising is not limited to money transferred immediately to a fraudster.

A fraudulent advertisement may initiate a chain of events involving identity theft, compromised accounts, misuse of personal data, unauthorised financial arrangements, invalid insurance, unnecessary contractual liabilities, inflated claims costs and repeat targeting.

Victims may also be placed on lists identifying them as responsive to scams. This can lead to recovery fraud, where a further fraudster offers to recover the original loss in return for another payment.

Cost displacement

Online platforms receive revenue from paid advertising, but much of the cost of detecting, investigating and disrupting fraudulent advertising is borne elsewhere. Those costs may fall on victims, insurers, financial institutions, regulators, law enforcement and legitimate businesses whose brands have been impersonated.

The impact assessment should recognise:

- investigative costs incurred by insurers;
- costs of supporting misdirected or affected consumers;
- brand protection and monitoring costs;
- claims leakage associated with misleading claims and accident management activity;
- law-enforcement and regulatory costs; and
- the wider effect on insurance premiums and consumer confidence.

Speed of harm

The assessment should place greater weight on the speed with which an advertisement can cause harm. A fraudulent advertisement may reach a substantial number of users before a conventional report, review and appeal process has concluded. Speed should therefore be treated as an element of severity when determining proportionate controls and removal expectations.

Under-reporting by businesses

Ofcom rightly identifies consumer under-reporting. There is also likely to be material under-reporting by affected businesses. Reporting systems can be slow, inconsistent and difficult to navigate. Businesses may repeatedly report advertisements using their identity without receiving sufficient information about the outcome or action taken against related accounts.

This creates an incomplete picture of the volume of fraudulent advertising and the resources being committed by legitimate businesses to disrupt it.

Do you agree with the examples of risky characteristics we have provided? Please provide any arguments and supporting evidence

Yes. The examples provide a useful foundation, particularly impersonation, unusual URLs, cloaking, GenAI-generated content, dramatic changes in account behaviour and abnormal advertising spend.

However, the indicators should be expressly non-exhaustive and capable of rapid updating as fraud typologies develop. Providers should be expected to consider indicators collectively and across linked accounts, rather than requiring any one characteristic to be conclusive.

The following additional characteristics should be included:

- an advertiser purporting to sell, arrange, introduce or promote insurance without clear authority to do so;
- use of insurer branding, trademarks, policy documents, employee names or claims terminology by an unverified third party;
- search advertising triggered by combinations of insurer names and terms such as ‘claim’, ‘accident’, ‘telephone number’, ‘contact’, ‘recovery’ or ‘repair’;
- a mismatch between the advertiser’s identity and the organisation named in the advertisement or landing page;
- domains which closely imitate the domain of an insurer, broker or regulated firm;
- recently created or frequently changed domains;
- landing pages which change materially after approval;
- requests to move quickly to private messaging services;
- multiple advertisements sharing telephone numbers, payment routes, URLs, devices or administrator details;
- unusually cheap insurance offers;
- testimonials, quotations or policy documents that purport to come from insurers but cannot be authenticated;
- rapid replacement of banned accounts;
- use of dormant or previously unrelated accounts to advertise financial or insurance products;
- frequent changes to account ownership, administrator permissions or payment details;

- unusual geographical inconsistencies between account location, target audience, payment source and purported business address;
- a high volume of materially similar advertisements placed through multiple accounts;
- previous reports from the impersonated business, an insurer, the Insurance Fraud Bureau, law enforcement or another recognised expert body; and
- advertising presented as an official insurer claims route where the beneficial operator is a lead generator, claims management company, accident management company or other third party.

Ofcom should also distinguish between indicators visible within advertisement content and indicators available only to the provider. Consumers and affected businesses will not usually have access to device identifiers, historic administrator details, payment data or links between accounts. Providers should be expected to use that information proactively.

Approach to codes

Do you agree with our proposed approach? Please provide any arguments and supporting evidence

Keoghs agrees with the layered and safety-by-design approach. Account controls, fraud indicator assessments, moderation and reporting should reinforce one another.

However, an iterative approach must not become a reason to defer effective obligations. The present consultation has already taken a significant period to reach this stage, while fraudsters continue to adapt rapidly. The first Codes should therefore contain sufficiently clear, measurable and enforceable minimum standards from the outset.

We recommend that the final Codes:

1. set clear implementation dates;
2. include defined expectations for urgent reports;
3. require preventative action before high-risk advertisements are published;
4. require investigation of linked accounts and infrastructure;
5. establish ongoing, rather than one-off, advertiser verification;
6. include measurable outcomes and reporting requirements; and
7. provide for rapid regulatory intervention where systems repeatedly fail.

The Codes should focus on outcomes, not merely whether a process exists. A provider should not be treated as having an effective system simply because it has a reporting form, moderation team or written policy. Ofcom should assess whether the system reduces exposure, acts quickly, detects repeat actors and prevents recurrence.

Providers should publish meaningful data addressing:

- the number and proportion of advertisements subject to verification;
- proactive detection rates;
- reports received from users, businesses and trusted flaggers;
- median and longest response and removal times;
- account suspensions and advertising bans;
- repeat-offender and linked-account detection;
- appeals and reinstatement outcomes; and

- recurrence associated with previously identified advertisers, domains or infrastructure.

Combined impact assessment

Do you consider the overall burden on the service providers in scope of our proposed measures to be proportionate? Please provide any arguments and supporting evidence

Yes. The burden is proportionate given:

- the scale and severity of fraudulent advertising;
- the reach and resources of the Category 1 and Category 2A services concerned;
- the advertising revenue generated by those services;
- the control providers exercise over access to their advertising systems;
- the informational advantage providers have over consumers and affected businesses; and
- the costs currently displaced to victims, insurers, law enforcement and legitimate organisations.

The inconvenience or cost of additional verification should be weighed against the potentially life-changing effects of fraud. Properly designed verification can also protect legitimate advertisers from impersonation and improve confidence in online advertising.

The proportionality assessment should take account of the provider's role in creating the risk and its ability to prevent it. Where a provider benefits financially from advertising and controls access to its service, it is reasonable to expect it to fund effective preventative systems.

Volume 2: Risk, Governance and Control

Advertising intermediaries

Do you agree with our proposal? Please provide any arguments and supporting evidence

We agree with the principle that providers should take action where advertising intermediaries are used. However, "insufficient control" should not become a broad exemption.

A provider choosing to use an intermediary should be required to take all reasonable steps to ensure equivalent standards apply throughout the advertising pathway. This should include contractual requirements, audit rights, data-sharing provisions, performance monitoring and a power to suspend an intermediary that cannot demonstrate effective controls.

Ultimate responsibility for the safety of advertisements displayed on the service should remain with the provider.

We have included two illustrative examples of when and how this measure may be applied, and what 'all reasonable endeavours' might look like. Do you have any comments on these examples, and do you have any additional examples of how providers could work with or require intermediaries to implement safety measures in circumstances where they have insufficient control? Please provide any arguments and supporting evidence

"All reasonable endeavours" should require active and evidenced intervention. It should not be satisfied merely by inserting general compliance wording into an agreement.

Additional examples should include requiring intermediaries to:

- identify the advertiser and beneficial operator;
- verify authority to act for the organisation being advertised;
- retain verification records;
- disclose relevant advertiser, domain and payment information promptly;
- screen against shared blocklists and high-risk indicators;
- notify providers of changes to account ownership, domains or landing pages;
- suspend advertisements where urgent fraud intelligence is received;
- prevent a banned advertiser from re-entering through another intermediary;
- support audits and testing by the provider; and
- demonstrate compliance through regular data and performance reports.

Where an intermediary repeatedly supplies fraudulent advertisements, fails to provide essential information or cannot prevent previously banned advertisers returning, reasonable endeavours should include restricting or terminating that relationship.

Fraud indicator assessment

Do you agree with our proposal? Please provide any arguments and supporting evidence

Yes. A fraud indicator assessment is essential, but it should operate as a live control framework rather than a periodic compliance document.

The assessment should:

- be informed by actual incidents and external intelligence;
- identify emerging typologies;
- distinguish between sectors and products;
- examine linked networks rather than isolated accounts;
- inform pre-publication controls;
- be reviewed following serious incidents or material changes;
- produce documented actions and accountable owners; and
- be tested against outcomes.

Ofcom should require providers to demonstrate how the assessment has changed their systems. It should not be sufficient simply to catalogue known risks.

Do you think there are other information sources providers should consider in order to understand how fraudulent advertising manifests on their service? If so, what information and why would they need to consider it?

Yes. Providers should consider information from:

- law enforcement (including the Online Crime Centre and Report Fraud UK);
- the National Fraud Intelligence Bureau;
- the Insurance Fraud Enforcement Department;
- the Insurance Fraud Bureau;
- insurers and regulated financial services firms;
- the FCA and other regulators;
- consumer organisations;
- recognised brand protection and cyber-security specialists;
- domain registrars and hosting providers;
- telecommunications providers;
- financial institutions and payment providers;
- complaints and redress bodies;
- advertising standards bodies;
- academic and independent research; and
- the provider's own historic enforcement, payment, device and account data.

The insurance industry holds valuable information about ghost broking, policy manipulation, paid ad spoofing, suspected fraud networks, copied documents, false claims routes and impersonation of insurers.

Information sharing should be reciprocal wherever lawful. At present, insurers and other affected businesses may provide intelligence to a platform but receive little information about linked campaigns, action taken or recurrence. A more mature system would allow trusted partners to identify emerging typologies and receive sufficient feedback to improve collective prevention.

Effective intelligence-sharing should ultimately support enforcement as well as detection. While the proposed Codes place significant emphasis on identifying and removing fraudulent advertisements, there should also be greater clarity around how intelligence is escalated to regulators and law enforcement to support action against the individuals and organised networks responsible. In our experience, the removal of individual advertisements or accounts alone is often insufficient. Fraudsters frequently re-emerge using new accounts, domains, identities and payment methods, creating a persistent 'whack-a-mole' cycle. The success of the regime should therefore be measured not only by the amount of content removed, but also by its ability to facilitate disruption of repeat offenders and support criminal, regulatory or civil enforcement action where appropriate. Ofcom should work closely with law enforcement, regulators and industry bodies to ensure that actionable intelligence generated through these measures contributes to meaningful consequences for those committing fraud, rather than simply the removal of the latest manifestation of their activity.

Governance and accountability

Do you agree with our proposals? Please confirm which proposed measure your views relate to and provide any arguments and supporting evidence

Yes. Our comments relate to proposals for senior accountability, reporting, oversight and review.

Fraudulent advertising should be treated as an enterprise-wide safety risk, not solely as a content moderation issue. Responsibility should extend across advertising, product design, engineering, security, payments, legal, compliance and senior management.

The accountable senior individual should have:

- sufficient authority and resources;
- access to relevant performance information;
- responsibility for remedial action;
- oversight of intermediaries;
- visibility of repeat-offender trends; and
- a duty to escalate systemic failures.

Board or senior-management reporting should be based on risk and outcomes, including recurrence, removal times, linked-account detection, trusted-flagger performance and the effectiveness of preventative controls.

Ofcom should be able to distinguish between an isolated operational error and a systemic failure arising from inadequate investment, weak governance or a business model which prioritises advertising volumes over safety.

Testing advertisement generation tools

Do you agree with our proposal? Please provide any arguments and supporting evidence

Yes. Providers should test advertisement generation tools before launch and throughout their operation.

Testing should include attempts to generate:

- advertisements impersonating insurers or regulated firms;
- false claims of FCA authorisation;
- fabricated insurance documentation;
- cloned branding and websites;
- offers of unrealistically cheap insurance;
- advertisements redirecting users to suspicious domains or private messaging services;
- deepfake endorsements; and
- variations designed to evade known detection controls.

Testing should not be confined to whether the tool itself produces the final advertisement. It should also examine how generated content can be combined with provider targeting, optimisation and distribution tools.

Where vulnerabilities are identified, providers should be required to address them promptly, document the mitigation and retest its effectiveness. Evidence of testing and material findings should be available to Ofcom.

Providers should also use AI and machine learning defensively to identify suspicious similarities, linked infrastructure and rapid reappearance of banned campaigns. Human review remains important, particularly where decisions are contested or context matters.

Volume 3: Ensuring Account Integrity

Account checks and actions

Do you agree with our proposal? Please provide any arguments and supporting evidence

Yes. Strong account integrity controls are fundamental. The most effective point of intervention is before an advertiser is permitted to place content.

Verification must be substantive rather than superficial. Confirming that an organisation exists is not the same as confirming that the advertising account holder is authorised to act for it.

Providers should also consider the relationship between the advertiser, organisation, domain, landing page, payment method, administrators and any regulated status claimed.

Where your feedback relates to a specific check we are proposing providers should carry out, please make this clear by responding in the corresponding box. These are:

a) Verification that advertising account holders work for, or on behalf of, the individual or organisation they are advertising

We strongly support this check.

Providers should verify both identity and authority. For insurance advertising, this should include whether the advertiser is genuinely authorised to sell, arrange, introduce or promote the product or service concerned.

Verification should not rely solely on an email address or document supplied by the advertiser. Providers should use a combination of reliable evidence and, for higher-risk sectors, independent confirmation using contact information obtained separately from the applicant.

Where an agency or intermediary is involved, the provider should confirm the relevant client mandate and the identity of the ultimate beneficiary.

b) Checks and actions to prevent banned account holders returning

We strongly support this proposal. It is central to addressing the present ‘whack-a-mole’ problem.

Controls should examine linked:

- identities
- administrators;
- devices;
- IP and network information;
- payment methods;
- telephone numbers;
- domains and landing pages;
- business addresses;
- agencies and intermediaries; and
- advertisement content and creative assets.

Providers should not treat a newly created account as unrelated simply because it uses a different account name.

c) Checks for accounts with indicators that there is a material risk they will post fraudulent advertising so that restrictions can be applied to them

We agree. Restrictions should be proportionate but capable of preventing content being published while risk is assessed.

High-risk advertising should be subject to enhanced verification and, where appropriate, pre-publication review. Financial services and insurance advertising, brand impersonation indicators, recently created domains and links to previously banned infrastructure should be treated as relevant risk factors.

d) Repeat checks where there are relevant changes identified on an account

We agree. Relevant changes should include:

- ownership or administrator changes;
- new domains or landing pages;
- a change of payment method;
- a material change in advertised products;
- abnormal advertising spend;
- a sudden change in geography or audience;
- dormant accounts becoming active;
- unusual login behaviour; and
- intelligence from an affected business or trusted source.

High-risk accounts should also be subject to periodic re-verification even where no single triggering event has been identified.

Are you aware of any other account checks and actions providers could do to protect users from fraudulent advertising? Please provide arguments and supporting evidence

Providers should:

- verify beneficial ownership and controlling persons;
- verify ownership of associated domains;
- confirm claimed regulatory permissions;
- screen for links with previously banned accounts;
- monitor material changes to landing pages after approval;
- require stronger authentication for high-risk advertising accounts;
- limit advertising functionality pending completion of enhanced checks;
- retain evidence supporting verification;
- notify the legitimate organisation where its identity appears to be impersonated;
- apply campaign-wide restrictions where multiple related accounts are identified; and
- investigate agencies or intermediaries associated with repeated fraudulent advertising.

Providers should also preserve information for lawful disclosure to regulators and law enforcement. Prompt preservation is important because fraudsters may delete accounts or infrastructure after detection.

Preventing fraudulent financial services advertising

Do you agree with our proposal? Please provide any arguments or supporting evidence

Yes. Financial services advertising presents a heightened risk because consumers may lose significant sums, enter damaging agreements or provide sensitive personal information.

However, checking that a named business appears on a regulatory register is insufficient. Providers should verify that:

- the advertiser is the regulated firm or is authorised to act for it;
- the advertised activity falls within any relevant permissions;
- the contact details and domain correspond with the genuine firm;
- the firm has approved the advertisement where required; and
- the advertisement does not falsely imply an association with another regulated entity.

Insurance should be expressly included in supporting examples, including ghost broking, clone firms and paid ad spoofing.

Countering account takeover

Do you agree with our proposal? Please confirm which proposed measure your views relate to and provide any arguments or supporting evidence

Yes. Our comments relate to account security, detection of suspicious changes and action following suspected takeover.

Account takeover allows fraudsters to inherit the history and apparent legitimacy of an established account and may enable them to bypass onboarding controls. Providers should therefore monitor for sudden changes in administrators, credentials, location, devices, payment methods, advertised products, URLs and spending patterns.

High-risk changes should trigger step-up authentication, temporary advertising restrictions and review. Providers should also ensure that recovery processes cannot themselves be manipulated by fraudsters.

Do you have any evidence about account takeover that could inform our assessment, including how frequently it occurs or its impact?

Keoghs does not currently hold consolidated quantitative evidence which would allow us to estimate the overall frequency of advertising account takeover.

Our experience nevertheless supports Ofcom's assessment that takeover of established or dormant accounts can be particularly harmful because the account may initially appear legitimate and may bypass controls aimed principally at newly created accounts.

The impact can include consumer loss, misuse of legitimate payment details, reputational damage to the genuine account holder and rapid dissemination of fraudulent advertisements before the change is detected.

Advertising bans

Do you agree with our proposal? Please provide any arguments and supporting evidence

Yes. A ban should apply to the fraudulent actor and relevant connected advertising infrastructure, not simply to the individual account used to place one advertisement.

Providers should investigate linked accounts and preserve relevant evidence. Bans should also be shared across services operated by the same provider where lawful and proportionate.

Ofcom should monitor whether banned advertisers are returning and require providers to report repeat-offender rates. A high rate of rapid return would indicate that the control is not effective.

Are you aware of any additional exceptional circumstances in which it may be proportionate for providers to reverse advertising bans?

A ban may be reversed where there is reliable evidence that:

- the account was taken over without the legitimate holder's involvement;
- the account was incorrectly linked to a fraudulent actor;
- the decision resulted from a material factual or technical error; or

- control has been restored to the legitimate business and appropriate security measures have been completed.

The burden should be on the appellant to provide sufficient evidence. Reinstatement should not occur merely because a different administrator, payment method or business name has been supplied.

Where a genuine account was compromised, reinstatement should ordinarily be accompanied by enhanced monitoring and re-verification.

Account appeals

Do you agree with our proposal? Please confirm which proposed measure your views relate to and provide any arguments or supporting evidence

Yes. Our comments relate to the availability, independence and timeliness of appeals.

Appeals are important to protect legitimate businesses, particularly where automated systems produce false positives. However, an appeal should not automatically permit advertising to resume where there is a material risk of fraud.

Appeal reviewers should have access to the full basis for the original decision, including linked-account and security information. They should also be appropriately trained in relevant fraud typologies.

Providers should monitor appeals for coordinated abuse, including multiple nominally separate businesses submitting materially identical evidence or relying on the same representatives.

Volume 4: Moderation

Advertising moderation

Do you agree with our proposal? Please confirm which proposed measure your views relate to and provide any arguments or supporting evidence

Yes. Our comments relate to proactive detection, resourcing, training, removal and review of linked content.

Moderation must operate before publication as well as after publication. Post-publication removal alone cannot adequately protect consumers where advertisements can reach large audiences quickly.

Moderators should receive sector-specific training, including on:

- ghost broking;
- paid ad spoofing;
- clone firms;
- misleading claims and accident management advertising;

- brand impersonation;
- false regulatory claims;
- domain manipulation;
- account takeover; and
- phoenixing and linked-account networks.

Removal of an advertisement should automatically prompt consideration of associated accounts, campaigns, domains, payment methods and materially similar creative content.

Ofcom should adopt clear expectations for speed. Urgent reports from law enforcement, regulators, recognised trusted flaggers or an impersonated regulated business should be investigated immediately and actioned within a defined period, subject to any exceptional case requiring further assessment.

Terms of Service and publicly available statements

Do you agree with our proposal? Please confirm which proposed measure your views relate to and provide any arguments or supporting evidence

Yes. Our comments relate to clarity, accessibility and consistency between public statements and actual practices.

Terms should clearly explain:

- prohibited fraudulent advertising;
- advertiser verification requirements;
- the use of proactive detection;
- circumstances in which accounts may be restricted or banned;
- treatment of linked accounts;
- complaint and appeal routes;
- information retained following enforcement; and
- circumstances in which information may be shared with regulators or law enforcement.

Public statements should include measurable information about performance. High-level commitments to safety are of limited value without evidence of detection, response, removal and recurrence outcomes.

Advertising complaints

Do you agree with our proposal? Please confirm which proposed measure your views relate to and provide any arguments or supporting evidence

Yes. Our comments relate to accessibility, dedicated reporting channels, feedback and urgent escalation.

Reporting should be straightforward and should not require the reporter to make detailed legal assessments. A business whose brand is being impersonated should be able to report the advertisement, related account and associated domain in one process.

Reporters should receive:

- confirmation of receipt;
- a unique reference;
- an indication of the priority applied;
- notification of the outcome; and
- a route to escalate an inadequate or delayed response.

Dedicated channels should be available to regulators, law enforcement, the Insurance Fraud Bureau, the Insurance Fraud Enforcement Department, regulated firms and other bodies able to demonstrate relevant expertise.

Consideration should also be given to formalising trusted escalation pathways for recognised industry bodies. In the insurance sector, organisations such as the Insurance Fraud Bureau and the Association of British Insurers are often able to identify emerging fraud typologies, coordinated campaigns and repeated impersonation activity affecting multiple firms. A clear mechanism for escalating credible intelligence from such bodies could assist providers in prioritising urgent cases and taking faster action against repeat offenders.

Ofcom should set minimum service expectations. Without defined standards, the proposal risks reproducing existing reporting arrangements under which content can remain live while the affected business repeatedly attempts to secure action.

Ad libraries

Do you agree with our proposal? Please provide any arguments or supporting evidence

Yes. Effective ad libraries can support detection, research, investigation and accountability. They should include removed advertisements as well as currently active advertisements. Otherwise, the evidence necessary to understand a campaign may disappear when the advertisement is taken down.

Access should be free and searches should not require unnecessary account registration.

Do you agree with the principles, functionalities and information categories which we have included in the proposed measure? Please explain your reasoning and, if possible, provide supporting evidence

Broadly, yes. Libraries should allow searches by:

- advertiser and account;
- beneficiary or organisation advertised;
- date;
- target audience and location;
- domain and landing page;
- telephone number;
- key words;
- advertisement image or materially similar creative content;
- status, including removed or restricted;
- reason for removal, where publication is lawful and appropriate; and
- connected campaigns.

Each entry should preserve the advertisement as encountered by users, the advertiser identity disclosed to the provider, the period for which it was active, material changes made during the campaign and the ultimate enforcement outcome.

Providers should take care not to publish personal data unnecessarily. That should not prevent meaningful disclosure of business identities, campaign relationships and enforcement information.

We also recommend a public data set or reporting mechanism covering confirmed fraudulent advertisements and repeat typologies. This would assist businesses, regulators and researchers in assessing whether the Codes are producing meaningful change.

Do you have any evidence or insights on the process of building an ad library from scratch or adjusting an ad library to align with the proposed measure, and how long that process would take?

This is an area outside of our technical expertise.

We nevertheless consider that implementation difficulty should be assessed in light of the scale, resources and advertising capabilities of the Category 1 and Category 2A providers in scope. Any transitional arrangements should be limited and should not delay implementation of core verification, reporting, removal and account-integrity protections.

Annexes

Equality Impact Assessment and Welsh language assessment

Do you agree with our Equality Impact Assessment? Please provide any arguments and supporting evidence

Keoghs does not propose to comment in detail on the methodology of the Equality Impact Assessment, which is outside our specific expertise.

We agree that fraudulent advertising can affect people across society and that vulnerability may be situational rather than confined to a particular demographic group. Factors such as financial distress, bereavement, an accident, limited digital confidence or an urgent need for assistance may temporarily increase vulnerability.

In the insurance context, a motorist attempting to contact an insurer immediately following an accident may be particularly susceptible to a misleading paid search result. Accessibility and ease of reporting should therefore form part of the practical assessment of impact.

Do you agree with our Welsh language assessment? Please provide any arguments and supporting evidence

This is an area outside of our expertise.

We support the general principle that Welsh-speaking users should receive protections, reporting routes and safety information which are no less effective than those available in English.

Guidance on making fraudulent advertising judgements: updates to the Illegal Content Judgements Guidance

Do you agree with our Proposals? Please provide any arguments and supporting evidence

Broadly, yes. Guidance should recognise that providers have access to information which is not visible to users, affected businesses or external moderators. A judgement should therefore consider all information reasonably available to the provider, including account history, payment information, links with previously banned accounts, domain changes, reports from impersonated businesses and related enforcement activity.

The guidance should include insurance-specific examples, particularly:

- an advertisement purporting to offer insurance without evidence of authority;
- an account using genuine insurer branding but directing users to an unrelated domain;
- paid search advertising which falsely presents a third-party claims business as the consumer's insurer;
- a ghost broker showing purported policy documentation or quotations;
- an advertiser falsely claiming FCA authorisation;
- multiple accounts promoting the same insurance offer through shared contact details or payment infrastructure; and
- a previously banned advertiser returning through a new account.

The "reasonable grounds to infer" test should not be applied as though Ofcom or providers must establish the complete underlying fraud before protective action can be taken. The purpose of the regime is preventative. Where a combination of reliable indicators establishes a material and credible risk, providers should be able and expected to restrict the advertisement pending further investigation.

At the same time, the guidance should require providers to record the information relied upon and provide an effective appeal route for legitimate advertisers.

Conclusion

Keoghs supports the introduction of robust Fraudulent Advertising Codes of Practice. The proposed framework contains many of the right components, but its effectiveness will depend on speed, enforceability and whether it changes outcomes in practice.

In particular, Ofcom should:

1. finalise and implement the Codes as quickly as possible;
2. set defined response and removal expectations for urgent reports;
3. require meaningful advertiser identity and authority checks;
4. require ongoing monitoring and re-verification;
5. treat linked-account and network disruption as a core requirement;
6. recognise ghost broking and paid ad spoofing expressly in guidance;
7. strengthen reciprocal intelligence sharing with insurers and fraud bodies;
8. establish clear escalation and trusted-flagger pathways for insurers, the Insurance Fraud Bureau, the ABI and other recognised expert bodies;

9. ensure providers remain accountable where intermediaries are used;
10. require transparent and measurable performance reporting; and
11. take timely enforcement action where providers' systems repeatedly allow the same actors or infrastructure to return.

Effective enforcement will depend not only on the quality of platform controls but also on the ability of affected businesses and industry bodies to secure a rapid response when fraud is identified. Ofcom should therefore encourage clear escalation routes for trusted organisations able to provide credible evidence of impersonation, organised fraud activity or emerging threats. Faster escalation and action against repeat offenders is likely to deliver significantly greater consumer protection than the repeated removal of individual advertisements in isolation.

The success of the Codes should not be assessed simply by the number of advertisements removed. The more important measures are whether fraudulent advertisements are prevented from reaching consumers, whether known fraudsters are stopped from returning, and whether the time between detection and effective disruption is materially reduced.