Advertising Standards Authority (ASA) response to Ofcom Fraudulent Advertising Codes Consultation

1. Background and introduction

1.1 This submission is provided by the Advertising Standards Authority (ASA).

1.2 The ASA works alongside the self-regulatory Committee of Advertising Practice (CAP) and the Broadcast Committee of Advertising Practice (BCAP). Together with the arm's length funding body – the Advertising Standards Boards of Finance (Asbof) – these bodies comprise the 'ASA System.'.

1.3 The ASA is the UK's independent advertising regulator. We have been administering the non-broadcast Advertising Code (written and maintained by CAP) for over 60 years and the Broadcast Advertising Code (written and maintained by BCAP) for over 20, with our remit further extended in 2011 to include companies' advertising claims on their own websites and in social media spaces under their control.

1.4 We are the UK's independent frontline regulator of ads by legitimate businesses and other organisations in all media, including online. Our work includes undertaking proactive projects and acting on complaints to tackle misleading, harmful or offensive advertisements. We are committed to evidence-based regulation, and we continually review new evidence to ensure the rules and our application of them remain fit-for-purpose.

1.5 As the UK's frontline advertising regulator, the ASA brings together different statutory, co-regulatory and self-regulatory enforcement mechanisms so they appear seamless to people and businesses. Our system involves the active participation of a range of legal backstops in the consumer protection landscape. We work closely with a network of partners including the Medicines and Healthcare products Regulatory Agency, Competition and Markets Authority, Information Commissioner's Office, Ofcom, Trading Standards, the Gambling Commission and the Financial Conduct Authority.

1.6 We call our model of partnering with businesses and other regulators 'collective ad regulation.' The ASA's independence and the buy-in and support we receive through collective ad regulation delivers faster, more flexible, more joined-up and proportionate regulation.

1.7 The UK Advertising Codes include rules reflecting specific legal provisions and rules developed through a separate regulatory process, which in combination ensure ads don't mislead, harm, or seriously offend their audience. The inclusion of the rules in the UK Advertising Codes has enormous benefits for responsible businesses and for consumers, who benefit from the protection the rules and the ASA's application of them afford.

2. Overview of ASA Scam Ad Alert system

2.1 The ASA regulates ads published on behalf of legitimate businesses, and our system works because the advertising industry buys into it. That is not the case for actors with criminal intent, often based in non-UK jurisdictions, who place 'scam ads' to fraudulently secure money, personal information or other benefits. While we play an active role in seeking to disrupt scam ads via the ASA Scam Ad Alert system, we do not investigate the ads because criminals, who have no regard for the law, clearly have no incentive to comply with the UK advertising rules. The ASA, and the bodies that comprise the ASA system,

staunchly support tackling criminal actors through appropriately funded, sufficiently resourced and suitably empowered domestic and international law enforcement bodies.

2.2 We refer to both ‘scam ads’ and ‘fraudulent ads’ throughout this response. The ASA more commonly uses the term ‘scam ads’ because it is more likely to be meaningful to consumers. There is no single definition of ‘scam ads’, but for the purposes of our Scam Ad Alert system we define them as paid-for ads with a clear malign intent to deceive consumers into purchasing a product or service or handing over personal information.

2.3 When the ASA alerts online advertising service providers to a ‘scam ad’, we do so because we consider that the content of the ad, together with any other contextual information, suggests that the actor placing the ad may have malign intent and that action at account level, not just ad level, may be appropriate. We anticipate that many of the ads for which we send Scam Ad Alerts will in future also be classed as fraudulent advertising as defined by the Online Safety Act.

2.4 While we are not established, constituted or funded to formally tackle ad-related fraud in a broad sense, we do have a view specifically on online scam ads. The large scale of online fraud is challenging for those with specific powers or other means of leverage to address it. More needs to be done to tackle online fraud across a broad array of fronts. Tackling online scam ads is a global challenge, requiring a joined-up response primarily involving law-enforcement bodies, statutory regulators, and the platforms used by fraudsters. The wider online ad industry and national advertising regulatory bodies such as the ASA also have an important role to play.

2.5 In June 2020, we launched the ASA UK Scam Ad Alert system in partnership with major digital advertising and social media platforms to help play our role in disrupting ads that seek to scam consumers.

2.6 The services that participate in the Scam Ad Alert system include Google, Meta, X, Snap, TikTok and many others. It is a requirement of the IAB Gold Standard that, where relevant, certified buyers or sellers of digital media must be signed up to the ASA Scam Ad Alert system.

2.7 Consumers can report suspected scam ads appearing in paid-for space online to us via an online form. We assess reports within 24 hours. If we judge that an ad is very likely to be a scam, we promptly send an Alert to all participating companies with key details of the scam ad, as well as to publishers when the ad appeared on a publisher owned site. If they locate them, partners remove the offending ad and may suspend the advertiser's account. In some instances, they may also add the account holder or associated URLs to blocklists, even when the ads weren’t appearing on their platform, stopping similar ads from that account or associated accounts from appearing in future. We expect the platform on which the ad originally appeared to give us an assurance within 48 hours that the ad is no longer appearing.

2.8 We share all alerts with the National Cyber Security Centre (NCSC). They operate the government’s takedown service, which seeks to remove malicious email addresses and websites. They scan the Alert for website addresses (URLs) to find the host website and remove it if it’s found to be malicious. This means that alerts not only result in action against the ads but, in some cases, also the websites they link to, which increases their effectiveness in protecting consumers.

2.9 We consider that reporting from bodies such as the ASA and other organisations recommended as trusted flaggers has an important role to play in identifying individual scam ads, identifying broader trends in scam advertising and holding services to account.

Volume 1: Context

Online advertising ecosystem

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

The information within this section of the consultation reflects the ASA's understanding of the workings of the online advertising ecosystem, to the best of our knowledge.

In reference to 'boosted content' at 3.10 and 3.11, we note that the judgement of whether such content is likely to be considered user-generated content appears to be complex. However, in practice the ASA has not come across this as presenting a barrier in work on scam ads.

Regarding blocklists (3.36), the ASA has previously seen evidence that while blocklists can help, they are not sufficient on their own to prevent harmful ads from appearing. In a report on harmful in-app ads, we saw examples of non-compliant ads still appearing despite multiple parties having moderation and content controls in place.[1] Note that this report did not relate to scam advertising.

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.

We share Ofcom's concerns regarding both the direct impact of fraudulent advertising on consumers and the wider impact on audience trust in legitimate advertising.

We agree with the breadth of fraudulent advertising types identified in the consultation, all of which we recognise from ads reported through the ASA's Scam Ad Alert system. It is important to recognise that breadth because appropriate mitigations may vary considerably between different scam types. For example, mitigations aimed at addressing the use of deepfakes and celebrity endorsements are likely to be particularly relevant to certain investment scams, whereas different interventions may be needed to tackle retail scams.

We agree that fraudulent advertising can have a detrimental impact on trust in online advertising more generally. Our experience is that consumers frequently report concerns not only about the specific ad encountered but also about how such ads were able to appear on well-known platforms or alongside legitimate advertising.

We also agree with Ofcom's observation that fraudulent advertising techniques evolve rapidly. Through the Scam Ad Alert system we have seen the types of scams, products,

[1] https://www.asa.org.uk/static/0ba66802-5d44-443b-a54d27c651176670/Online-ad-supply-pathway-of-in-app-ads-that-harmfully-objectify-women.pdf

services, public figures and brands used by fraudsters change over time, often in response to current events and technological developments.

Some categories of fraudulent advertising may present more difficult judgement calls than others. In particular, for some types of potentially fraudulent retail advertising there can be a less distinct boundary between advertising that is clearly fraudulent and advertising that is misleading but not necessarily fraudulent. This may present challenges both for regulators and for services when determining what content should be reported, investigated or removed. Ofcom may therefore wish to consider any mechanisms or further guidance to help establish the boundaries of what content falls within the scope of fraudulent advertising, as opposed to advertising which may be misleading but is not fraudulent, beyond that already presented in the updates to the Illegal Content Judgements Guidance. That clarity is important given both the potential consequences for advertisers where content is reported as suspected fraudulent advertising, including the impact on these advertisers' freedom of commercial speech, and the potential for consumer harm if fraudulent advertising is not removed.

One example is certain 'dropshipping' retail websites that claim to be based in the UK but are in fact located abroad and facilitate deliveries direct from China. Such dropshippers often falsely claim that they have been established for many years in Britain and that they are family businesses making hand-crafted products, an impression supported by AI-generated imagery. In the past, dropshippers often did not include real contact addresses on their websites, which was a clear breach of our Code and legislation and supported swift enforcement action. However, we have more recently observed advertisers in this space registering virtual offices or using unrelated real addresses, with the effect that the advertising may appear more legitimate while the identity of the business behind it remains difficult to establish.

Another example is companies, some seemingly based in Europe, that target scam devices at UK consumers, such as energy saving plugs that "will cut 99.7% off your bill", or USB sticks that allow access to all paid-for streaming services for free. These are registered companies that appear to be legitimate but advertise widely on social media with AI-generated videos making unsubstantiated or scientifically impossible claims, and deliver products that are cheap, ineffective and sometimes unsafe.

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

Advertising content risky characteristics:

Impersonation through content – We agree with the risky characteristics set out in this section relating to celebrities, public figures and brands.

A significant proportion of Scam Ad Alerts issued by the ASA relate to scam ads exhibiting these characteristics[2], and this has been the case since the launch of the Scam Ad Alert system in 2020[3]. The particular celebrities and public figures featured in scam ads vary over time, although some individuals, such as Martin Lewis, remain persistently popular with scammers. Others, including politicians, fluctuate over time.

[2] https://www.asa.org.uk/news/a-year-in-scams-2025-scam-ad-alert-update.html

[3] https://www.asa.org.uk/news/asa-scam-ad-alert-system-update-on-numbers-and-trends.html

Brand impersonation also remains a persistent feature of fraudulent advertising. Examples range from misuse of established news brands such as the BBC and ITV to lend credibility to fabricated news stories through to ads falsely claiming to sell products on behalf of well-known retailers or brands. The brands involved also change over time. For example, we have observed ads exploiting the closure of well-known retailers by claiming to offer heavily discounted closing-down stock.

We commonly observe multiple impersonation techniques being used together, for example the use of a celebrity image, a fake news article and branding associated with a well-known publisher. The presence of multiple forms of impersonation within the same consumer journey can be a particularly strong indicator of fraud.

Unusual URLs – We agree that this is a risky characteristic. In our experience, this can be particularly significant where an ad claims to originate from a specific brand, retailer, news organisation or public body, but the destination URL bears no obvious relationship to that organisation.

This characteristic is likely to be most useful when considered alongside other indicators, as legitimate advertisers may also use campaign-specific domains or alternative URLs.

Investment and cryptocurrency advertisements – We agree that this is a significant risky characteristic. A substantial proportion of Scam Ad Alerts relate to ads which either directly promote investment or cryptocurrency opportunities or link through to landing pages that do so.

Investment and cryptocurrency scams represent only one category of scam advertising, however. It is therefore important that mitigations are capable of addressing a broad range of scam types.

Use of GenAI and deepfakes – We agree that this is a risky characteristic when AI is used in the manner described in the consultation.

As noted in the consultation, the ASA has observed an increase in reports relating to deepfake ads[4]. In our experience, AI-generated content is often an evolution of existing scam types, particularly celebrity endorsement scams and investment scams, rather than creating entirely new forms of scam advertising.

Exaggerated, attention-grabbing and pressure-inducing content – We agree that this can be a useful supporting indicator when observed alongside one or more other risky characteristics.

In isolation, however, it is a less specific characteristic. Nearly all fraudulent ads are designed to attract attention in some way and many seek to create a sense of urgency. However, many legitimate ads also seek to attract attention or encourage consumers to act quickly.

Similarly, exaggeration may feature in some fraudulent ads but is also a characteristic of some ads that may be misleading rather than fraudulent. In our experience, this characteristic is most useful when combined with other indicators of fraud.

Cloaking – We agree that this is a significant risky characteristic and one that is particularly associated with some types of scam advertising. Cloaking is especially significant because it

[4] https://www.asa.org.uk/news/a-year-in-scams-2025-scam-ad-alert-update.html

undermines automated review processes and makes it more difficult for platforms and regulators to assess the true destination and content associated with an ad.

Advertising account risky characteristics:

Suspicious behaviour – We agree that the indicators described in this section are risky characteristics, although our knowledge is limited to where public information is available about account behaviour, which varies between services.

Through our Scam Ad Alert work we have observed examples of accounts that appear to have undergone multiple name changes before posting scam ads, which may indicate account compromise or attempts to conceal previous activity. We have also observed instances where recently created accounts have been used to advertise products or services while simultaneously claiming that the advertiser is long-established or well-known.

We also consider that indicators of potential account compromise may be relevant. Some scam ads appear to originate from accounts that previously displayed legitimate activity before switching to promoting scam content.

Impersonation through accounts – The ASA has received reports relating to ads placed by accounts that appear to impersonate well-known brands, retailers and public figures. In some cases, the account name itself closely resembles the brand or individual being impersonated. In others, even where the account name (where publicly available) is unrelated, the branding within the ad can create an overall impression of affiliation with an organisation or individual when no such relationship exists. That can extend to the landing page and the URL.

We also anticipate that advances in AI-generated content may further increase the sophistication and credibility of impersonation attempts.

Approach to Codes

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

We support the proposed approach. In particular, we welcome the layered approach and the emphasis on account-level interventions. Our experience suggests that effective action against scam advertising often requires intervention not only against individual ads but also against associated advertiser accounts and other accounts running materially similar scam ads.

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.

Based on our experience of the harms associated with scam advertising and the challenges involved in tackling it effectively, the ASA's view is that the measures appear proportionate and appropriately targeted.

We particularly note the importance of ensuring that systems and processes are effective in practice and capable of evolving in response to changing fraud typologies. Given the dynamic nature of this threat, we consider that a degree of ongoing investment and adaptation by services is likely to be both necessary and proportionate.

Volume 2: Risk, Governance and Control

Advertising intermediaries

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

The ASA agrees with the proposed intermediaries measure.

We support Ofcom's objective that the use of advertising intermediaries should not result in weaker protections for users or create gaps in the application of the Fraudulent Advertising Codes. The complexity of online advertising supply chains should not reduce the effectiveness of measures intended to protect users from fraudulent advertising. We agree that providers should remain responsible for achieving equivalent safety outcomes regardless of the advertising pathway used to place ads on their services.

We particularly support:

- the principle that providers should use "all reasonable endeavours" where they have insufficient control to apply a measure directly; and
- the expectation that providers work with, or require, intermediaries to implement equivalent protections.

As referenced in the consultation, the ASA's experience through the Intermediary and Platform Principles Pilot provides practical evidence that platforms and intermediaries can work together to support regulatory objectives across the advertising supply chain.

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.

The ASA considers both examples useful and reflective of how advertising supply chains operate in practice to our knowledge. The moderation example is particularly helpful because it recognises that providers may not always have direct visibility of the ad being served but should nevertheless take reasonable steps to ensure moderation is carried out.

Through the ASA's Intermediary and Platform Principles Pilot[5], buy-side and supply-side online businesses voluntarily adhered to Principles to

- **promote the CAP Code and the ASA** to advertisers, agencies and people who see advertising online;
- **signpost advertisers to platform targeting tools**, helping advertisers meet their responsibility to direct age-restricted advertising towards adults and away from children;
- **act on repeated non-compliance**, including removing non-compliant ads from recidivist advertisers when notified by the CAP Compliance team; and
- **support ASA investigations**, including by helping the ASA obtain information relevant to suspected breaches of the CAP Code.

It would be a stretch to characterise these Principles as 'safety measures'. In each case, the online business has autonomy and control in its application of the Principles, which are designed to support the production, distribution and control of advertising to ensure

[5] https://www.asa.org.uk/resource/intermediary-and-platform-principles-pilot-final-report.html

advertising remains compliant with the UK Advertising Code. These businesses have, we understand, very limited ex ante or ex post liability for controlling – entirely or partly – the creative content that advertisers choose to adopt in their ads or the audience they choose to direct their ads to. Through the Principles, therefore, online businesses apply ex ante principles (see first two bullet points above) and ex post principles (see latter two bullet points above) to mitigate non-compliant ads coming to market and address ads which the ASA has determined to be non-compliant but where the advertiser refuses to suitably amend or withdraw the ad.

Fraud indicator assessment

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

The ASA supports the proposed fraud indicator assessment measure.

We welcome Ofcom's recognition that providers should develop and maintain an understanding of how fraudulent advertising manifests on their services and that indicators of fraud will evolve over time. We also welcome the emphasis on identifying new fraud indicators and adapting systems and processes accordingly.

We also support the requirement that between assessments providers should track new indicators of fraudulent advertising and feed these indicators into trust and safety processes as appropriate. We consider that those actions should be taken promptly when new indicators are identified.

We support the requirement that services working with intermediaries seek data about fraudulent advertising from those intermediaries to feed into the assessment. We consider that such information should also be sought on an ongoing basis, not only as part of the assessment process. For example, where an intermediary identifies a fraudulent ad, providers could require intermediaries to share relevant intelligence about associated advertiser accounts with them or information about relevant content indicators. Measures that facilitate intelligence-sharing and repeat-offender detection across supply chains are likely to improve outcomes.

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?

N/A

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.

The ASA supports the proposed governance and accountability measures.

We agree that there should be appropriate senior oversight and accountability for compliance with the fraudulent advertising duties and for implementation of the measures contained within the Codes.

We welcome the emphasis on effectiveness reviews. Governance arrangements should not focus solely on process compliance but should support continuous improvement, learning from fraud trends and adaptation to new scam techniques.

Testing advertisement generation tools

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

The ASA agrees with the proposal.

We support Ofcom's objective that providers should test ad generation tools to identify vulnerabilities that may be exploited by fraudsters and take appropriate action to address those vulnerabilities.

As advertising technologies become increasingly sophisticated, including the growing use of artificial intelligence and automated content-generation tools, there is a risk that such tools could be misused to facilitate fraudulent advertising at scale. We therefore welcome the focus on proactive testing and mitigation.

The ASA's Scam Ad Alert experience indicates that emerging technologies are increasingly being incorporated into scam advertising, including the use of AI-generated content.[6]

Volume 3: Ensuring account integrity

Account checks and actions

Do you agree with our proposal? Please provide any arguments and supporting evidence. Where your feedback relates to a specific check we are proposing providers should carry out, please make this clear. These are:

a. verification that advertising account holders work for, or on behalf of, the individual or organisation they are advertising;

b. checks and actions to prevent banned advertising account holders returning;

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; and

d. repeat checks where there are relevant changes identified on an account.

The ASA supports the proposed account checks and actions measures. We welcome Ofcom's focus on account integrity and the recognition that effective action against fraudulent advertising requires interventions upstream at account level as well as action against individual ads.

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

We support this proposal.

A significant proportion of scam ads reported to the ASA involve some form of impersonation of brands, retailers, media organisations or public figures. Verification measures of this nature should help reduce opportunities for bad actors to misrepresent themselves as affiliated with entities they do not represent.

b. Checks and actions to prevent banned advertising account holders returning

We support this proposal.

[6] https://www.asa.org.uk/news/a-year-in-scams-2025-scam-ad-alert-update.html

Our experience suggests that scam advertising frequently involves accounts continuing to run such ads following removal and other accounts running similar ads, indicating that the accounts may be linked. Measures designed to identify and disrupt repeat offenders are therefore likely to play an important role in reducing consumer exposure to fraudulent advertising.

c. Checks for accounts with indicators that there is a material risk they will post fraudulent advertising

We support this proposal.

Applying proportionate restrictions in response to risk indicators has the potential to reduce harm before fraudulent ads are widely seen by users. We agree that the landing page for the ad should be a relevant consideration as this is often essential to determine whether an ad is fraudulent or not. The landing page and wider website also frequently contain red flag indicators of potential fraud, such as T&Cs and privacy policies missing information.

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

We support this proposal.

In our experience, some scam advertising appears to be associated with changes to account characteristics, including account names.

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

On services that allow the public to review businesses or submit public comments on their pages, reviewing that content can indicate whether the public consider the business to be a scam operator. The ASA will often review that information and cite it in reports to platforms where relevant, although we would not rely on it as a sole indicator.

Preventing fraudulent financial services advertising

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

The ASA broadly supports the proposal but considers that Ofcom should clarify how the measure applies to financial promotions that are not required to be approved by an FCA-authorised person. We understand that the proposed wording may be intended to allow services to adopt stricter policies where they consider that appropriate. However, without further clarification, the current wording could lead to uncertainty for legitimate firms, platforms and regulators about which financial products or services fall within scope and what verification is expected.

Scam financial services ads, particularly those relating to investments and cryptocurrency opportunities, remain a significant category of scam ads reported through the Scam Ad Alert system. Measures designed to reduce the prevalence of such advertising therefore have the potential to deliver meaningful consumer protection benefits. We also support approaches that reduce opportunities for bad actors to exploit the credibility associated with regulated financial services.

Scope of measure

Within the financial services verification measure, Ofcom proposes two options for platforms. Either (1) to restrict advertising of financial services to those firms which are FCA-authorised, or (2) to also allow those ads which have been approved by an FCA-authorised firm or which

fall under an exemption in the Financial Services and Markets Act 2000 (Financial Promotion) Order 2005.

The first option would exclude firms that can legitimately advertise such as SRA-regulated law firms and IPAs (along with many others), which fall under the exemption.

The second option would enable those firms to advertise. However, there is a lack of clarity regarding those companies that do not need to be FCA authorised but also do not need to fall under the exemption to be able to advertise legally. This includes ads for tangible investments, as well as investments for crypto that don't fall under the FCA's qualifying cryptoassets requirement, such as NFTs. It may also be that some lead generation would fall under this category.

For example, investments for tangible assets such as gold, art, wine and whisky are not required to be FCA regulated. Businesses may legitimately offer such investments and ads for them should not be assumed to be fraudulent. However, ads for such unregulated investments do present particular risks for consumers as they are not subject to the protections afforded by the Financial Services Compensation Scheme or the Financial Ombudsman Service. The ASA has investigated ads for unregulated investments on that basis.[7] The current wording might lead to an outcome where services read it to mean that they need to verify that the advertiser is on the FCA register for all investment ads. This would prohibit any ads for unregulated investments even where they do not require FCA authorisation. It is not clear that is the intention. In that scenario we would foresee a lack of clarity for regulators, including the ASA, when considering issues relating to ads for such products or services.

Ofcom may therefore wish to consider clarifying the scope of the financial services measures and, additionally, whether ads for financial products and services that do not require FCA authorisation should be subject to any additional scrutiny by services, given the additional risks they present.

Definition of "financial product or service"

The consultation includes this definition in Annex 7:

"Any paid-for advertising that promotes, or is capable of promoting, financial products or services. This includes advertising for common types of financial services and products, including, but not limited to, investments, credit and loans, insurance, pensions, debt advice, and qualifying cryptoassets. The term 'financial services advertisements' is to be read accordingly."

There are services which wouldn't clearly come under this definition but may be regarded as being a type of financial service, such as tax services, tax claim/repayment agent services, certain accident management services, all of which the ASA has taken action against in the past. Although most concerned misleading advertising, there have been a small number (e.g. in accident management) that may be regarded as fraudulent advertising. We also note

[7] Example of recent ruling: https://www.asa.org.uk/rulings/cap-group-inc-ltd-a26-1329629-capgroup-int-ltd.html

claims management is not included in the list. Most types are FCA regulated or would fall under the exemption for legal firms.

Countering account takeover

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

The ASA supports the proposed measures to counter account takeover.

Our experience suggests that some scam ads appear to originate from accounts that previously displayed legitimate behaviour before switching to promoting scam content. Measures designed to identify, prevent and respond to account compromise are therefore likely to be beneficial.

We have observed examples where account behaviour suggested that previously legitimate accounts may have been compromised before being used to disseminate scam advertising. This has included apparent changes in account identity, branding or activity patterns immediately prior to scam ads being promoted.

We also see examples of old and unused accounts being taken over where it would be less likely that the legitimate owners would report them or even know they were being misused.

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

N/A

Advertising bans

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

The ASA supports the proposal.

We consider that it is proportionate to impose advertising bans where fraudulent advertising has been posted and that account-level interventions are necessary to prevent repeat offending.

We also support the principle that such measures should be proportionate and supported by appropriate safeguards.

Our experience of reporting suspected scam ads is that even where individual ads are removed, accounts may continue to post very similar ads. Some platforms will usually only remove the individual ads we report. Others will proactively remove other ads from the same account which are active at that point. However, it is not unusual for us to see those same accounts then posting the same ads afterwards. This leads to us having to report multiple ads over a period of days or weeks.

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

N/A

Account appeals

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

The ASA supports the proposed account appeal measures.

We agree that appeal mechanisms are an important safeguard and help ensure that account-level interventions remain proportionate and accurate.

Volume 4: Moderation

Advertising moderation

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

The ASA broadly supports the proposed advertising moderation measures, in particular the emphasis on proactive identification of fraudulent advertising, the requirement for providers to review ads they have reason to suspect may be fraudulent, and the expectation that providers should not rely solely on user reports to identify such content.

We welcome the proposal that providers set performance targets relating to both timeliness and accuracy. The ASA's Scam Ad Alert system involves timeliness targets: we aim to assess reports of suspected scam ads within 24 hours and ask platforms to provide an assurance within 48 hours that the scam ad has been removed (both excluding weekends). In 2025 platforms met this timeframe 96% of the time, demonstrating that swift assessment and action of reports is achievable.[8]

While we support the overall approach, we consider Ofcom could strengthen the measures by placing greater emphasis on the use of intelligence to identify and act against substantially similar ads once fraudulent advertising has been identified. A recurring issue identified through the ASA's Scam Ad Alert system is that individual ads are removed but are rapidly replaced by materially identical ads from the same or other advertising accounts. We consider that providers should seek to use intelligence obtained through moderation activity, trusted flagger reports and other sources to identify and take action against substantially similar fraudulent ads (even if they are not posted by accounts linked to the original fraudulent advertiser) and associated advertiser networks. We anticipate this may be addressed in the autumn consultation on using proactive technology but consider that it is important that expectations on platforms in this area are made clear.

Terms of service and publicly available statements

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

N/A

Advertising complaints

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

The ASA supports the proposed advertising complaints measures and, in particular, the proposed trusted flagger arrangements. We welcome Ofcom's proposal to include the ASA on the minimum list of recommended trusted flaggers, recognising that the ASA's experience

[8] https://www.asa.org.uk/news/a-year-in-scams-2025-scam-ad-alert-update.html

operating the Scam Ad Alert system provides relevant expertise in identifying some fraudulent ads.

We support the proposal that providers establish and maintain dedicated reporting channels for trusted flaggers and that reports submitted through those channels should amount to a reason to suspect that an ad may be fraudulent.

It would be helpful for trusted flaggers if, where possible, providers give reasons if they disagree with the assessment of a trusted flagger that an ad was likely to be fraudulent. We recognise that this may sit outside the scope of the proposed measure, which aligns closely with Ofcom's guidance. However, feedback from providers would support effective engagement between trusted flaggers and services by enabling trusted flaggers to provide further information, refine future reports or otherwise engage constructively with the service. At present the ASA does not always receive reasons in the relatively infrequent instances where reported ads are not removed.

Ad libraries

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

The ASA supports Ofcom's proposal to require providers to establish and maintain ad libraries.

The ASA agrees that ad libraries are an important tool to support the detection and reporting of suspected fraudulent advertising. We make extensive use of ad libraries in our relevant work, both to identify potential scam ads, and to obtain further details of ads reported to us to allow us to make an accurate assessment of the ads in question. Where they are unavailable or have less functionality, we are significantly limited in our ability to investigate and detect potentially fraudulent or scam ads.

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.

We believe certain aspects of the proposed functionality are essential for the utility of ad libraries:

- Robust search functionality as proposed
- An API that should allow full access to the contents of the ad library and does not impose technical restrictions such as low request rate limits or other technical barriers that unduly restrict legitimate usage
- Advertising account name and advertiser name
- The content of the ad – which must be both complete and an accurate representation of how the content was presented to end users
- Landing page URL as part of the ad content information – this is often essential to be able to determine whether the ad is fraudulent or not
- Actual reach – allows for proportionate response and prioritisation by the reporter of ads that reach large numbers of people
- Ad status – allows for prioritisation by the reporter of ads that are still active

Existing ad libraries have mixed functionality and quality, with many not implementing all of the characteristics described above.

We believe it is also important that providers reasonably promptly resolve any issues with the ad library they are made aware of.

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?

N/A

Annexes

Equality Impact Assessment and Welsh language assessment

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

N/A

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

N/A

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.

We agree with the fraudulent advertising-specific guidance proposed. In particular, we welcome the fact that the draft annex reflects the distinct characteristics of paid-for advertising and the types of information and intelligence that may be available to providers when assessing whether an ad is fraudulent.

We welcome the proposed red flag indicators relating to impersonation of brands, companies and public figures, including use of usernames or account names that may be mistaken for legitimate entities and use of branding or the likeness of a person where characteristics of the advertising account are inconsistent with the entity being represented.

As previously referenced, a significant proportion of scam ads reported through our Scam Ad Alert system involve false claims of endorsement by public figures, misuse of well-known brand identities, or ads that seek to create the impression of affiliation with a legitimate business.

We also welcome Ofcom's recognition that providers should consider contextual and reasonably available information when assessing ads and should not assess content in isolation. We agree that fraudulent advertising judgements should be made with reference to all information that is both relevant and reasonably available.

We particularly welcome the recognition of the relevance of landing page and destination website information when assessing suspected fraudulent advertising, including through references to landing page content and URL-scanning technologies. We strongly support this approach. The ASA's experience is that many scam ads cannot be accurately assessed by considering the ad content in isolation. Overt indicators of fraud often appear primarily on landing pages. We therefore consider that providers should consider landing page and destination information wherever it is reasonably available to them (including when it is provided in a report from a trusted flagger), as this is frequently where key indicators of fraud become apparent.

As noted in our response on the causes and impacts of fraudulent advertising, some categories of fraudulent advertising may present more difficult judgement calls than others. In particular, for some types of potentially fraudulent retail advertising there can be a less distinct boundary between advertising that is clearly fraudulent and advertising that is misleading but not necessarily fraudulent. This may present challenges both for regulators and for services when determining what content should be reported, investigated or removed. Ofcom may therefore wish to consider any mechanisms or further guidance to help establish the boundaries of what content falls within the scope of fraudulent advertising, as opposed to advertising which may be misleading but is not fraudulent. That clarity is important given the potential consequences for advertisers where content is reported as suspected fraudulent advertising, including the impact on these advertisers' freedom of commercial speech. We provide more specific examples in our response above.

At 13.17 reference is made to the fact that "Most paid-for online advertisements that are misleading but not fraudulent may be subject to potential enforcement action by the ASA, including financial marketing communications that are not regulated by the FCA." Enforcement action can also be taken by other bodies including the CMA and Trading Standards. We would therefore suggest reference is added to those bodies, particularly given their statutory powers.

2 October 2026