# Your response

## 1. Background and Introduction

1.1. This submission is provided by the Advertising Standards Authority (ASA), the Committee of Advertising Practice (CAP) and the Broadcast Committee of Advertising Practice (BCAP) – the 'ASA system.'

1.2. 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 19, with our remit further extended in 2011 to include companies' advertising claims on their own websites and in social media spaces under their control.

1.3. 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.

1.4. We work closely with a network of partner regulators including Ofcom, the Gambling Commission, the Information Commissioner's Office, the Medicines and Healthcare products Regulatory Agency, the Financial Conduct Authority and the Competition and Markets Authority. Our frontline ad regulation often complements their activities, or even frees them up entirely to concentrate on their other duties. Through the sharing of information, joined-up enforcement action and referral processes, our partners bolster our regulation and assist us, where necessary, to bring non-compliant advertisers into line.

1.5. We also bring together the ad industry and media owners to set, maintain and police high standards. The UK Advertising Codes are drafted and maintained by the industry committees of CAP and BCAP, supported by experts in our Regulatory Policy team. This means businesses have a direct stake and an enlightened self-interest in adhering to the standards they set and creating a level-playing field amongst them.

1.6. The UK Advertising Codes include rules reflecting specific legal provisions and rules developed through 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 afford.

1.7. There are multiple checks and balances in place to ensure the committees' development of rules and guidance is transparent, open to scrutiny and adheres to the principles of good regulation. These include calls for evidence and public consultations; mandatory regard to the advice of an expert independent consumer panel; Ofcom signing off on BCAP rule changes; the ASA System's processes being open to judicial review and more besides. All to ensure the system is wholly accountable to everyone with a stake in advertising.

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

1.9. In addition to investigating ads, we also provide a wealth of training and advice services (most of which are free) for advertisers, agencies, and media to help them understand their responsibilities under the Codes and to ensure that fewer problem ads appear in the first place. CAP and BCAP provided over a million pieces of advice and training in 2023.

## 2. The ASA's remit and role in online regulation

2.1. The ASA regulates the content and targeting of advertising. Primary responsibility for observing the Code falls on marketers. The CAP Code states that others involved in preparing or publishing marketing communications, such as agencies, publishers and other service suppliers, also accept an obligation to abide by the Code.

2.2. There is an effective online advertising regulatory framework in place in the UK to protect people, in particular children, young and vulnerable people from harm. With more than 60 years' experience regulating advertising, the ASA provides a one-stop shop for consumers and for the industry across all media and platforms. We regulate almost all advertising online, including paid ads on platforms and the open internet, influencer ads, and companies' own website and social media advertising claims. (The exceptions are political advertising and misleading-related issues in non-broadcast financial advertising, which falls to the FCA.)

2.3. The ASA regulates advertising by legitimate businesses and is not the appropriate body to tackle ads by criminal actors who are often based in non-UK jurisdictions, although we do contribute to the disruption of scam ads in paid-for space online via our Scam Ad Alert system. We're fully supportive of the aims of Online Safety Act and, where we have role and remit (protecting children from harmful or inappropriate content, and adults from legal but harmful content) we will use the tools at our disposal to protect consumers.

2.4. Moreover, under our new *AI-assisted collective ad regulation* strategy we will continue to undertake proactive, tech-assisted, collective regulation to tackle irresponsible ads at scale and speed.

2.5. Our role is to ensure that the content of ads seen by UK consumers, including those appearing online and in social media, follows the Advertising Code. The enduring principles of the advertising rules are that ads must not mislead, harm or offend and should be prepared in a socially responsible way. We also require that ads are targeted responsibly and are appropriate for the audience that sees, hears and engages with them.

2.6. The standards we apply through the Codes are, almost without exception, the same for broadcast advertising and for non-broadcast advertising, including online. That is in no small measure because many of the rules directly or indirectly reflect law that applies across media.

2.7. The ASA system sets specific standards for content and placement of advertising, including on a sectoral or thematic basis. For example, ads for alcohol, gambling and HFSS food and drink are all subject to placement rules, while advertising rules on misleadingness seek to reflect consumer protection regulation.

2.8. As mentioned in 1.4 and 1.5 the ASA operates a system of collective regulation. We also have a long established and strong co-regulatory partnership with Ofcom. Ofcom is our statutory backstop for broadcast advertising and co-regulator for Video On Demand / Video Sharing Platforms. We stand ready to build on that relationship in relation to any advertising issues that might emerge from its new role as the Online Safety Regulator. Through better intelligence sharing, referral processes, joint sector compliance work and joined-up enforcement action, our regulatory partners bolster our regulation.

# Volume 5: How to judge whether content is illegal or not?

## The Illegal Content Judgements Guidance (ICJG)

| **Question 49:** |
| --- |
| i) Do you agree with our proposals, including the detail of the drafting? |

We have focussed our response below on section *A6. Fraud and other financial offences* pages 77-90 of the ICJG as that is the section which is relevant to the ASA's operation of its Scam Ad Alert system.

**Overview of ASA Scam Ad Alert system:**

The ASA regulates ads published on behalf of legitimate businesses, and our system works because the advertising industry buys into it. This is obviously not the case with criminals, often based in non-UK jurisdictions, placing illegal scam ads. While we play an active role in seeking to disrupt scam ads, we do not investigate them because criminals, who have no regard for the law, clearly have no incentive to comply with the UK advertising rules. The ASA system staunchly supports, however, the tackling of criminal actors via appropriately funded, sufficiently resourced and suitably empowered domestic and international law enforcement bodies.

While it is not our role or remit to speak about fraud in a broad sense, we do have a view specifically on scam ads online. The scale of online fraud is challenging for regulators. More needs to be done to tackle online fraud across a broad array of fronts. Tackling online scam ads is a global problem, requiring a joined-up response involving law-enforcement bodies and statutory regulators, platforms and all involved in the online ad industry, as well as national advertising regulatory bodies such as the ASA.

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

The ad platforms, networks and other companies who participate in the Scam Ad Alert system include Google; Meta (Facebook/Instagram); Taboola; Outbrain; Microsoft; TikTok; Yahoo; Snap; Twitter; Amazon Ads; Sizmek Ad Suite; RevContent; Index Exchange; Clean.io; Reach; and the Media Trust, LinkedIn and others. It was recently added as a requirement of the IAB Gold Standard that, where relevant, members must be signed up to the ASA Scam Ad Alert system.

For the last four years, consumers have been reporting scam ads appearing in paid-for space online to us via an online form.

If we judge that an ad is a scam, we promptly send an Alert to all participating platforms 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 them to blocklists, even when the ads weren't appearing on their platform, stopping them from appearing in future.

We also share all alerts with the government's 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 also the websites they link to, which increases their effectiveness in protecting consumers.

We assess reports within 24 hours, enabling us to quickly and effectively alert platforms to scam ads so that they can promptly remove them, suspend the advertisers' accounts and stop similar ads 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. Given the harms of scam ads and that we know scammers often cycle through individual ads quickly we consider it is important that platforms act at speed when provided with actionable intelligence. All participants signed up to the system on that understanding.

We continue to monitor the performance of our system and work collaboratively with stakeholders to play our part in tackling scam ads online.

**Comments on scope of the guidance:**

We understand that the ICJG will apply, as will the rest of the provisions consulted upon, to user generated content (UGC) and search services and that there is no exemption for paid-for services from UGC. Consequently, some ads which are within the remit of the CAP Code will also be subject to the requirements of the OSA, including non-paid for advertising (eg. non-paid for posts advertising a product or service), influencer advertising and paid-for advertising, where it meets the definition of UGC. However, this is not currently set out in the documents.

Whilst most of the guidance in this consultation phase relates to offences which are outside of the ASA's remit, as set out above the ASA operates a Scam Ad Alert system for online paid-for ads which are clear cut scams. Our understanding is that the scope of the Scam Ad Alert system is therefore likely to include some content which will also fall within the scope of the ICJG, for example where the user of an in-scope service places a paid-for ad on that site.

In our view it would be beneficial if Ofcom were to share more detailed guidance and definitions on content which is both within and outside of scope, particularly in relation to content which we consider to be advertising (including non-paid-for, paid-for and influencer), with specific examples where possible.

We understand that a further consultation will take place on fraudulent advertising later in the year, regarding content on certain services which is not already in scope as UGC.

**Comments on the content of the ICJG:**

The relevant section of the ICJG lists the relevant priority fraud and other offences and provides guidance to in-scope services on how they might determine if a specific piece of content is likely to amount to an offence.

The offence most relevant to the ASA's Scam Ad Alert system is likely to be fraud by false representation. However, it is important to be clear that when assessing reports of potential scams the ASA does not directly consider them in relation to any specific fraud offence. The ASA defines scam ads within the scope of the Scam Ad Alert system as: paid-for online ads with a clear intent to deceive consumers into purchasing a product or service that either doesn't exist, or is falsely misrepresented, or to hand over personal information. Such ads will in practice nearly always be in breach of ad networks' own policies.

Not within scope of the Scam Ad Alert system are: non-paid-for ads; issues which the ASA would normally investigate (such as whether an ad from a business which appears to be legitimate is misleading, harmful or offensive); copyright disputes; counterfeit goods; non-online content.

In our experience, in most cases it is straightforward for our experienced staff to determine if a reported ad is a scam or not.

For example, many scam ads reported to us use a common approach of an ad featuring fake celebrity news or an endorsement, and then link through to a fake news article giving further detail, before finally linking through to a page where personal details are solicited. These scams are often termed 'FizzCore' and frequently use 'cloaking' to disguise the landing page. Cloaking is a sophisticated camouflage technique designed to evade automated detection, where malicious creatives and landing pages are hidden from certain users. Common product/service types being advertised in scam ads using fake celebrity news or endorsements include cryptocurrency scams, weight loss pills and CBD gummies.

We have also seen a recent trend for ads which falsely claim to be from established retail brands. These are also straightforward to assess because it is evident that the landing page is not for the claimed retailer.

When we send a Scam Ad Alert we set out that the ad breaches: Consumer Protection from Unfair Trading Regulations, 2008; and UK Ad Code (CAP Code) Rule 3.1 ("Marketing communications must not materially mislead or be likely to do so"). We also explain precisely why we consider that specific ad to be an obvious scam ad, for example that it features a fake celebrity endorsement and links through to a fake news article. We provide more detailed examples further down.

There are some scenarios where it is less clearcut whether an ad is a scam or not. For example, where 'too good to be true' claims are being made for a product there is a judgement call to be made as to whether an ad is a scam or whether it might instead not meet that threshold but could nonetheless be misleading. In the latter scenario we might instead choose to investigate via our formal investigation route and give the advertiser an opportunity to respond. A recent example of ads which we considered fell into this grey area was ads for mini-heaters, where we sent Scam Ad Alerts for those with the strongest claims and formally investigated others. Further information about those rulings can be found on our website here.

We consider it likely that some ads which we consider to be clear-cut scams and send Alerts for would not meet the threshold set out in the guidance, as it is currently drafted. The most obvious example is where a post does not in itself contain a request, invitation or inducement to invest or send money (etc). We would be concerned if an impact of the guidance was that in-scope services no longer considered they therefore needed to remove such content. We therefore suggest that consideration is given as to how that risk can be mitigated.

The ASA does not have access to the full range of information which in-scope services will have available, for example IP addresses or details of user flags. However, we have nonetheless considered and commented below on the three groups of indicators provided at A6.37 onwards.

Regarding Group 1, some of the example indicators align with indicators that the ASA would highlight in Scam Ad Alerts where relevant. For example: *"Use of an account or page which claim to represent a public figure, well known organisation or brand, unless it is obviously run as a parody".* The ASA commonly receives reports about copycat ads which falsely claim to be from a particular brand or company. Sometimes the whole account will use a 'copycat' name. In other cases the account name will relate to something else entirely, but the ad will make a false claim to represent or feature an endorsement by a public figure, well known organisation or brand. Ofcom therefore may wish to consider broadening out the reference from account to ad/post level.

Regarding group two, A6.39 states that *"Services should next consider whether the content in question contains a request, invitation or inducement to invest or send money, monetary instruments or digital assets (e.g. gift cards, crypto currency, in-game currency/items etc.), or to send other private financial or identification information, such as bank documents, bank details or identification documents".* All of the examples given relate to the content of the post itself, or other on-site content. The ASA does see some examples of scam ads which fall into this category. However, many ads which the ASA consider to be scams do not contain any such request, invitation or inducement. For example, we see many examples of ads which contain false sensationalist headlines about celebrities which then link through to a series of websites where the user is eventually encouraged to submit their details to take advantage of a potential investment opportunity (e.g. crypto-related) or to sign up to a product subscription (e.g. For weight loss pills, CBD gummies, etc). Our understanding is that as part of compliance processes platforms will often undertake measures to check the content of webpages which ads link to, and for the ASA the content of the website an ad links to is a vital step in determining whether the ad itself is a scam or not. Ofcom therefore may wish to consider whether the content of websites which posts link to should also be referenced in the guidance.

Regarding group three, A6.41 refers to an example of the *"use of apparently deliberately misspelt words to evade automated filters (e.g. '0ne million d0llars')"*. The ASA regularly sees examples of scam ads taking that approach so would endorse that example. Another technique utilised by scammers to avoid detections is to use "non-printable characters", which are read as characters by the computer but are not displayed to the user.

Something else we observe on some platforms is legitimate accounts (including those belonging both to celebrities and members of the public) which appear likely to have been hacked then being used to post scam ads. We consider that it is likely that platforms will have access to indicators regarding hacked accounts and that such indicators should be considered for inclusion in the guidance.

Other indicators not currently listed in the guidance that the ASA considers when determining if an ad is likely to be a scam or not include:

- Trustpilot reports on the advertiser – these can give an indication as to whether a company or website may be a scam, for example if a large proportion of reviews report it being a scam, not having received a product, or the product being nothing like that advertised
- Public comments on the ads themselves, where that function is available. For example if a large proportion of reviews report it being a scam, not having received a product, or the product being nothing like that advertised
- Highly unrealistic discounts and/or prices within the ads or the landing pages
- Highly unrealistic product specific claims, for example dramatic weight loss claims for weight loss supplements or implausible energy savings claims for mini-heaters
- Online publicly available reports from other regulators or consumer bodies – these might relate to a type of scam or a particular company or website
- Indicators specific to the content of the website which the ad links through to:
    - Extensive use of stock images
    - Phone numbers or unusual phrases in ads also appear on other suspicious websites – our experience is that scammers tend to copy and paste the same information over multiple sites
    - T&Cs don't refer to the name of the company.
    - Contact addresses connected with virtual offices/Mail Box Etcs
    - Links to countries with known links to organised crime
    - Non-operative HTTPS certificate (by checking the padlock next to the URL)
    - No contact details
    - Fake contact address
    - Fake company registration number
    - Fake endorsements/accreditation
    - Fake trustmarks. Many security companies offer these (e.g. McAfee Secure, TRUSTe, Verisign), and they are designed to be clicked on to provide additional security information. If they are just image files, they are almost certainly fake.
    - No privacy policy/T&Cs or privacy policies/T&Cs obviously copy and pasted from elsewhere - references to unrelated companies etc

As with the indicators listed in the ICJG none of the indicators above are decisive in our judgement of whether an ad is an obvious scam, but in combination they provide evidence for our decision-making process.

**Examples of recent scam ads:**

By way of illustrating how we judge in practise whether an ad is a scam or not, below are some examples of recent ads which we have sent Scam Ad Alerts for. We have set out underneath each example the factors which led us to conclude the ad was a scam:

1. A paid-for ad from an account on a social media site which featured an image of a well-known celebrity and a caption which referenced "shocking" news. The ad contained a link to what appeared to be to the BBC website to "Read it now".

- The 'news' referenced in the ad did not relate to real events.
- The ad linked through to a fake BBC news article.

2. Five paid-for ads from an account on a social media site which offered various products (including a jacket, perfume and hair curlers) for £9.

- The landing page where you could purchase the products includes a compulsory bi-weekly subscription for around 50 Euros, which was not referenced in the ads.
- The Trustpilot page included reviews saying that it was a scam.
- One of the ads claimed the company had a 4.9 star rating on Trustpilot, which was not the case.
- There was clearly contradictory information in the ads regarded the location which they dispatched products from.

3. A paid-for ad from an account on a social media site which said that a well-known retail platform was selling 'mystery boxes' for £1 .

- The ad referenced a well-known retail platform and featured their logo, implying that the ad was from that brand or affiliated with them. However, they had no association with that platform and the ad did not link through to their site.

4. A paid-for ad from an account on a social media site which featured an image of a well-known celebrity and made claims that they were advising people to "take advantage of this opportunity" and that "an investment of £200 brings over £27,720 monthly".

- Both the ad and landing page falsely used a celebrity image and name to promote fake cryptocurrency automated software.
- The ad and landing paged promised highly unrealistic profits.
- The landing page linked through to a fake Mirror news article.

5. A paid-for ad from an account on a social media site which featured an image of a package of bank notes and encouraged people to click to join a group chat.

- The ad linked to a Telegram page which referenced fake bank notes and cloned cards, inviting people to join a chat, where they were likely to request money or investment.

6. A paid-for ad from an account on a social media site which featured a video of DIY tools and claimed that a well-known DIY store was unable to sell them and so was giving them away for £2.

- The price for the product in the ad was highly unrealistic.
- The landing page was not for the well-known DIY store referenced in the ad but did use their logo.
- Rather than selling the product the landing page instead offered a survey to supposedly have a chance of winning the advertised tools.

7. A paid-for ad from an account on a social media site which featured text which referenced losing "three inches off my waist in a month without exercise or other lifestyle changes".

- The ad linked through to a landing page which featured fake testimonials from well-known celebrity investors supposedly promoting keto products.
- The efficacy claim made for the product in the ad was highly unrealistic.

ii) What are the underlying arguments and evidence that inform your view?

Response:

The ASA has operated the Scam Ad Alert system since 2020 and our experience doing so has informed our response above. In the 12 months to October 2023 the ASA processed 1877 reports of potential scams via our quick reporting form – we assessed swiftly whether they related to obvious scams in paid-for space online and included enough information for a Scam Ad Alert. As a result 152 Scam Ad Alerts were sent to platforms to remove ads and further act on intelligence. All major UK ad platforms and networks are signed up to the system and it is also a requirement of the IAB Gold Standard. As such, we are recognised in having expertise in assessing whether individual ads are scams.

See further information about the system on our website:

https://www.asa.org.uk/news/scam-ads-online-2023-update-on-our-scam-ad-alert-system.html

https://www.asa.org.uk/general/asa-scam-ad-alert-system.html

iii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: No

**Question 50:**

i) Do you consider the guidance to be sufficiently accessible, particularly for services with limited access to legal expertise?

Response:

We consider there is a risk that, due to its length and focus on complex legal tests relating to the various relevant criminal offences, services will find the guidance difficult to understand and to apply. There is a risk that the complexity will lead to inconsistency in the resultant decision making by services regarding individual pieces of content – for example, some may set the bar too high. We also note the lack of usage examples for the fraud offences. We consider that practical examples would be helpful for services.

| | |
|---|---|
| ii) | Please provide the underlying arguments and evidence that support your views. |

Response:

We have based our view above on our experience of developing internal guidance and expertise in assessing whether individual ads are scams, as well as our more general experience in producing guidance for advertisers.

| | |
|---|---|
| iii) | Is this response confidential? (if yes, please specify which part(s) are confidential) |

Response: No

**Question 51:**

| | |
|---|---|
| i) | What do you think of our assessment of what information is reasonably available and relevant to illegal content judgements? |

Response:

As per our answer to question 49, we suggest that Ofcom also considers whether the content of websites which ads link through to should also be considered reasonably available and relevant. As stated there, our understanding is that as part of compliance processes platforms will often undertake measures to check the content of webpages which ads link to, and for the ASA the content of the website an ad links to is a vital step in determining whether the ad itself is a scam or not.

| | |
|---|---|
| ii) | Is this response confidential? (if yes, please specify which part(s) are confidential) |

Response: No