Fraudulent Advertising Codes Consultation

Annexes 9 to 11: Proposed approach to guidance on making fraudulent advertising judgements and updates to the Illegal Content Judgements Guidance

Consultation

Published 10 July 2026
Closing date for responses: 02 October 2026

A9. Guidance on making fraudulent advertising judgements: updates to the Illegal Content Judgements Guidance

What is this section about?

This section explains our proposed approach to guidance on fraudulent advertising judgements, which we intend to publish as an annex to the Illegal Content Judgements Guidance. The guidance is intended to help service providers apply the Act's 'reasonable grounds to infer' threshold when assessing paid-for advertisements.

It also explains where our existing fraud guidance remains appropriate and where limited changes are needed to reflect the characteristics of paid-for advertising and the information likely to be reasonably available to providers.

This section is followed by:

- Annex 10: which shows proposed changes to Chapter 1 of the existing ICJG in mark-up; and
- Annex 11: which is the draft Fraudulent Advertising Judgements Annex and will become Annex 3 of the ICJG.

Our proposals

We propose to publish a Fraudulent Advertising Judgements Annex which adapts the existing fraud guidance, for paid-for advertising, including targeted offence-specific updates and cross-cutting guidance on reasonably available information. We also propose consequential updates to the ICJG to ensure consistency with the new annex and wider regulatory developments.

Why are we proposing these recommendations

We are proposing these recommendations because paid-for advertising has different characteristics from user-generated and search content, and providers are likely to have access to different information when assessing it. The proposals are intended to make the guidance clearer and more practical for fraudulent advertising judgements, while remaining consistent with the Act's legal threshold, the existing ICJG approach, and evidence on how fraudulent advertisements are encountered by UK users.

Consultation questions

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

Introduction

A9.1 This section outlines proposals regarding guidance on whether content is fraudulent advertising content, which we intend to publish by way of an annex to the Illegal Content Judgements Guidance (ICJG) to fulfil our duty under section 193(1) of the Online Safety Act 2023 (the Act).

A9.2 We refer to that annex throughout this chapter as the Fraudulent Advertising Judgements Annex. We include a draft version of this document at Annex 11 of this document. It will become Annex 3 of the ICJG.

A9.3 We published the ICJG as part of our December 2024 Illegal Harms Statement (our December 2024 Statement). The ICJG provides guidance to assist service providers when making illegal content judgements: that is, judgements as to whether search content or user-generated content (UGC) 'amount to' a priority offence or select non-priority offences. When making such judgements, a provider should consider if it has 'reasonable grounds to infer' that content is content of the kind in question (in this case, illegal content).[1] The ICJG includes a section on making illegal content judgements about the priority fraud offences set out in Schedule 7 to the Act.

A9.4 The draft guidance in the proposed Fraudulent Advertising Judgements Annex is intended to assist service providers to make judgements about whether paid-for advertising amounts to a fraudulent advertisement because it falls within one or more of the relevant fraud offences set out in section 40 of the Act ('fraudulent advertising offences'). We refer to judgements of this kind as 'fraudulent advertising judgements'. These are distinct from 'illegal content judgements' which refer to judgements about whether content is 'illegal content' for the purpose of providers' illegal content safety duties. The draft guidance includes information on the 'reasonably available information' which should be considered by providers as part of fraudulent advertising judgements.

A9.5 Where providers have reasonable grounds to infer that a paid-for advertisement amounts to a fraudulent advertisement, the advertisement in question should be considered to be fraudulent advertising as defined by the Act. Providers should take relevant action as required by the duties on fraudulent advertising set out in sections 38 and 39 of the Act.

A9.6 The Fraudulent Advertising Judgements Annex is particularly relevant to decisions about taking down such content or ensuring UK users are no longer able to encounter such content.[2] A fuller understanding of fraudulent advertising will also contribute to meeting broader aspects of those duties on preventing individuals encountering such content. Service providers can use the Fraudulent Advertising Judgements Annex and the consultation Volume 1, Section 4, 'Causes and impacts of fraudulent advertising' to

[1] 'Reasonable grounds to infer' is a threshold established by the Act. This threshold must be reached in order for content to be defined as illegal content or fraudulent advertising (see section 192(5) of the Act). According to section 192(5), the approach to be followed is whether a provider has reasonable grounds to infer that content is content of the kind in question (and a provider must treat content as content of the kind in question if reasonable grounds for that inference exist). Reasonable grounds for that inference exist in relation to content and an offence if, following that approach, a provider (a) has reasonable grounds to infer that all elements necessary for the commission of the offence, including mental elements, are present or satisfied; and (b) does not have reasonable grounds to infer that a defence to the offence may be successfully relied upon (section 192(6)). As we stated in our November 2023 Illegal Harms Consultation (our November 2023 Consultation), "what amounts to reasonable grounds to infer in any given instance will necessarily depend on the nature and context of the content being judged and, particularly, the offence(s) that may be applicable."

[2] Sections 38(1) and 39(1) for fraudulent advertising.

supplement their understanding of fraudulent advertising. This includes when implementing recommended measures in the Fraudulent Advertising Codes of Practice.[3]

Offence-specific proposals

A9.7 In the draft guidance, we are proposing to provide tailored guidance on the offences listed in section 40 of the Act only where this is necessary. Where a fraudulent advertising judgement need not differ from an illegal content judgement about the same offence, we have provided cross-references to reduce repetition.

A9.8 We are proposing to amend our guidance only where it is necessary to account for the differing characteristics of paid-for advertising content, or the differing types of information that is likely to be 'reasonably available' to service providers when considering this type of content.

A9.9 The remainder of this chapter explains our offence-specific proposals. We first address fraud by false representation, followed by financial services offences and articles for use in fraud. We are proposing that guidance on any offences not included in this section will remain the same as in the Fraud section of the ICJG.

Fraud by false representation

Examples of common false representations

A9.10 In our view, the majority of the examples of commonly encountered claims (or 'representations') given in the ICJG are still relevant. However, we are proposing to add two further examples, outlined in the paragraph below, which evidence shows can be encountered through paid-for advertising:

- a claim that a product (for example, a drug, medical product or weapon) is approved or legal to be sold in all circumstances in the UK (for example, without a licence or prescription), including by use of the logos or credentials of legitimately licensed companies or people; and
- a claim that the advertiser is authorised to advertise a product (where the ability to do so is restricted.

A9.11 We intend these examples to capture instances of advertisements being used to promote medication which is sold without prescription,[4] controlled drugs[5] and weapons which cannot be bought or sold legally in the UK (or cannot be bought or sold without an appropriate licence).[6]

Red flag indicator list

A9.12 In the ICJG we provided illustrative examples of 'red flag indicators' to assist service providers to identify content amounting to an offence of fraud by false representation. As part of the draft Fraudulent Advertising Judgements Annex, we propose to give similar guidance on the fraud by false representation offence, and to update the original list of red flag indicators as part of this to tailor it appropriately to advertising content. The changes

[3] See Volumes 2 to 4 for discussion of these proposed measures.
[4] Which?, 2025. Social media platforms are failing to block dubious health ads. [accessed 7 May 2026].
[5] Tech Transparency Project, 2025. Meta Allows Drug Ads Selling Everything from Opioids to Cocaine. [accessed 7 May 2026].
[6] Tech Transparency Project, 2024. From Glocks to Ghost Guns: Meta Approves Hundreds of Ads Selling Firearms. [accessed 7 May 2026].

reflect evidence we have seen about impersonation, account characteristics and indicators of user-generated content.

A9.13 Evidence submitted to us as part of our March 2024 Call for Evidence: Third Phase of Online Safety Regulation suggested that the impersonation of public figures and reputable firms is a tactic consistently employed by bad actors when posting fraudulent paid-for advertisements.[7] Accordingly, we propose to add the following red flag indicators to the sub-section, 'Information which suggests that the person submitting the advertisement is doing so dishonestly':

- use of a username or account name which is similar to, or able to be mistaken for, that of a username or account owned or operated by a brand, company or public figure; and
- use of the brand identity or the likeness of a person, where characteristics of the account submitting the advertisement are inconsistent with known characteristics of the brand or person concerned (for example, an account with an IP address outside the UK using the branding of a UK-based business in its advertisement in a way which suggests the product or service being promoted is associated with that business).

A9.14 We also consider it appropriate to replace the previous section in the 'red flag indicators' list on 'Technical anomalies or unusual user behaviour' with a section and indicator that is better tailored to paid-for advertisements.[8] This change will be made in the Fraudulent Advertising Judgements Annex only. We propose that the section should be titled 'Links to accounts that have been found to have posted fraudulent advertising to UK users'. We propose including the following red flag: "The advertising account submitting the advertisement shares identifiable characteristics with an advertising account that has already been identified as having posted a fraudulent advertisement. For example, the accounts may share the same phone number, IP address or device identifier, password, registered business address or residence, or named contact. However, service providers should always consider whether there is a legitimate explanation or reason for these similarities." However, we acknowledge that there may be legitimate reasons for common characteristics to be shared between accounts, and therefore propose to state in the Fraudulent Advertising Judgements Annex that providers "should always consider whether there is a legitimate explanation or reason for these similarities."

A9.15 We propose to change the indicator regarding claims that an "emergency has arisen", replacing it with claims that "an opportunity has arisen, and that quick action is required to benefit from it." While false emergency situations commonly feature in fraudulent user-generated content, evidence suggests that paid-for advertising content is more likely to create urgency by suggesting short supplies of products, for example, because of a closing-down sale.[9]

A9.16 We also propose to remove the following indicators from the red flag indicators list, as we consider them to be less directly relevant to advertising content:

- accounts which issue a high volume of posts, user connection or 'friend' requests, where: the majority of these are blocked or declined by other users; or such requests

[7] Financial Services Authority (FCA) response to 2024 Call for Evidence, p.4; Money Saving Expert response to 2024 Call for Evidence, pp. 24-5; Which? response to 2024 Call for Evidence, pp. 3, 4, 5 and 7.
[8] Evidence related to 'phoenixing' and 'lifeboating' can be found in Volume 3, 'Causes and impacts of fraudulent advertising' sub-section, 'Tools and techniques used in fraudulent advertising'.
[9] ASA, 2026. A year in scams: 2025 Scam Alert Update. [accessed 7 May 2026].

are persistently directed towards other users with whom the user concerned has no apparently connection, or to users in other countries; and

- a user who has purported to be a seller, but who stops responding to messages or blocks when a purchaser starts asking where the product is.

Contextual factors suggesting possible fraud by false representation

A9.17 We propose to make some changes in the presentation of how service providers should consider contextual factors, as laid out in A3.71 to A3.73 of the Fraudulent Advertising Judgements Annex (see paragraph 6.47 of Chapter 6 of the ICJG). We propose to change the wording used in paragraph 6.47, to clarify how providers should approach factors which often appear in advertisements or content amounting to fraud by false representation, but which also appear in legitimate advertisements or content, as these factors are not in themselves reasonable grounds for inferring fraudulence.

A9.18 We are not, however, proposing to change our substantive policy. We consider that it is still appropriate to position presence of these factors as a reason for prioritising review, or subjecting advertisements or content to further checks.

A9.19 For continuity, we propose to update paragraph 6.47 of the ICJG in a similar fashion.

Inferring dishonesty

A9.20 To add further clarity to the Fraudulent Advertising Judgements Annex, we propose to add examples of instances where it is reasonable to infer dishonesty from the contents of an advertisement itself.

A9.21 We recognise that behavioural signals can also play a role in supporting inferences about dishonesty. These signals may be different in the case of paid-for advertisements compared to when assessing UGC, particularly where judgements are being made before an advertisement goes live. Service providers could also revise judgements if they become aware that the advertisement or the landing page has been altered after it goes live and can be encountered by users. We therefore believe that limited, non-exhaustive examples can help providers to understand how drawing reasonable inferences about dishonesty may work in practice.

A9.22 We further recognise the prominent role played by marketing agencies ('agents') in online paid-for advertising. In some cases, advertisements may be submitted to a service's advertising platform by the person (including individual or company) whose products or services are being promoted. We refer to such people as 'advertisers'. However, providers are also likely to come across instances where an advertiser has contracted an agent to carry out its marketing activities, and this may include submitting an advertisement to a service's advertising platform on the advertiser's behalf.

A9.23 Advertising activity operates within a hierarchical structure[10] that can include different types of advertising accounts[11], such as corporate accounts and individual or manager advertising accounts. Advertising can be placed using "ad manager tools" integrated in a service or through multiple intermediaries. It can also be placed by media agencies working on behalf of advertisers. As such, we propose that the Fraudulent Advertising Judgements

[10]Advertisers may have multiple advertising accounts that can perform actions within an overall hierarchy, including a manager or parent account and individual accounts that perform specific actions. Advertising agencies can be contracted to carry out certain tasks, such as managing individual advertising campaigns and posting adverts.

[11] See Annex 7, Glossary for definition "advertising account holder".

Annex includes guidance to the effect that a service provider is not prevented from taking action on what it would otherwise have reasonable grounds to conclude is fraudulent advertising in cases where it is an agent who has submitted the advertisement to the service's self-service ad manager.

A9.24 We consider this to be a reasonable approach which accommodates the practical workings of the online advertising industry within the framework of fraud offences (which require the conduct and state of mind of a 'person'[12] to be reasonably inferred), while staying consistent with the overall intention of the Act to prevent users being exposed to fraudulent advertisements and the Act's legal threshold for fraudulent advertising (that is, reasonable grounds to infer that the content amounts to a fraudulent advertising offence).

Intent to make a gain or cause a loss

A9.25 In the case of paid-for advertising, it is our view that it is reasonable in most instances to assume that criteria related to "intention to make a gain or cause another person a loss" is satisfied by virtue of the advertisement being uploaded to a service's advertising platform. This is because, as stated in our draft guidance, "the ultimate purpose of most advertising is to encourage consumers to purchase goods or a service which will result in profit for a business or organisation, or to otherwise part with money or another form of value in some way to this same end."

A9.26 We recognise, however, that there may be instances where it is not appropriate to infer intent to make a gain or cause a loss in advertising content, such as public awareness campaigns. We therefore propose to include this caveat in our final guidance.

Use of artificial intelligence

A9.27 On artificial intelligence (AI), we propose to make minor amendments to the ICJG text which positioned the use of "edited, inauthentic or AI-generated images or celebrities" as a contextual indicator of fraud by false representation. Specifically, we propose to add the word 'decontextualised' to this list, to reflect the common use of images which have been taken out of their original context and re-presented to back up a false claim.[13] We also propose to add an explanatory footnote giving more detail on how advertisements may meet this description.

A9.28 We are aware that, since we published our December 2024 Statement, the use of generative AI in online content has increased rapidly. Our evidence shows that AI is also being used to generate paid-for advertising content either in part or whole.[14]

A9.29 While acknowledging this development, we propose to retain the original inclusion of "edited or inauthentic images, AI-generated images or celebrity images, which can be clicked on through an embedded hyperlink (taking users off-site) or are used conjunction with a link prompting users to move off site" as a contextual indicator of fraud by false representation. Framing this indicator as such means that it can be "useful in helping to identify an advertisement as a priority for review, or as needing further checks", but that it is in itself insufficient to indicate a false representation. We consider that this positioning

[12] Pursuant to section 236(1) of the Act 'person' includes (in addition to an individual and a body of persons corporate or unincorporate) any organisation or association of persons.
[13] Such imagery is sometimes referred to as a 'cheapfake' or 'shallow fake'. Source: Qian et al., 2023. Fighting cheapfakes: using a digital media literacy intervention to motivate reverse search of out-of-context visual misinformation, Journal of Computer-Mediated Communication, 28 (1). [accessed 28 April 2026].
[14] Ofcom, 2026. Behavioural audit of services with advertisement functionality

continues to be appropriate, given increased use of generative AI among bad actors as well as legitimate advertisers.

Financial services offences

A9.30 Three offences from the Financial Services and Markets Act 2000 (FSMA) are included in section 40 of the Act as fraudulent advertising offences. FSMA regulates the provision of financial services in the UK. It creates a number of activities which are subject to regulation and may only be carried out by authorised persons, including a regime specifically for the regulation of financial promotions (this applies to persons anywhere in the world promoting investments to UK users).[15] There are limited exemptions to the need to be authorised, focusing on specific types of financial services activity, and on specific individuals or firms carrying out authorised activities.

A9.31 Both here and in the Fraudulent Advertising Judgements Annex, we refer to the three FSMA offences in section 40 of the Act as 'the fraudulent advertising FSMA offences'. They comprise:

- false claims to be authorised or exempt;
- contravention of prohibition on carrying on regulated activity in the UK unless authorised or exempt; and
- contravention of restrictions on financial promotions.

False claims to be authorised or exempt

A9.32 We consider that our existing guidance in paragraphs 6.20 to 6.28 of the ICJG, regarding reasonable inferences about the offence of "making false claims to be authorised or exempt", also applies to fraudulent advertising judgements. As such, we propose no change to our approach.

Contravention of the prohibition on carrying out regulated activity unless authorised or exempt

A9.33 The ICJG did not provide substantive guidance on the offence of 'contravening the prohibition on carrying out regulated activity in the UK', focusing instead on the offence of contravening restrictions on financial promotions (the financial promotions offence). We consider that the same approach is appropriate in respect of fraudulent advertising judgements, and therefore propose no additional guidance.

A9.34 We are not aware of any evidence to suggest that authorised activities are carried out through paid-for advertisements on services in scope of the fraudulent advertising duties. For this reason, we propose to focus on the financial promotions offence only, as online advertisements are not commonly used to carry out regulated financial services activity.

Contravention of prohibitions on financial promotions

A9.35 The ICJG focused on the financial promotions offence, including inferences that may be drawn using information that is likely to be reasonably available to all providers, without the need for significant technical expertise. It stated that providers should conclude that an advertisement amounts to this offence in two scenarios:

[15] A financial promotion is content which seeks to persuade or incite the recipient to engage in 'investment activity' or engage in 'claims management activity' – both terms defined in law by FSMA.

- where the FCA or Prudential Regulation Authority (PRA) provides them with an explanation of why, in its opinion, each part of the FSMA fraudulent advertising offences concerned is present or satisfied;[16] and
- where a firm or individual can be identified as offering an investment, and this firm or individual appears on the FCA Warning List.[17]

A9.36 Reflecting the technical complexity of the FSMA offences in question, we stated that it would not be proportionate for the ICJG to say that the Act requires providers to "become sufficiently expert in UK financial services regulation to apply the FSMA offences correctly to the content they see." This, we stated, is due to the significant time and expertise that would be required to do so.[18]

A9.37 We propose to replicate the approach we took in the ICJG in the Fraudulent Advertising Judgements Annex. We note that replicating this approach does not prevent providers from continuing to moderate with reference to their own advertising policies (including policies which do not take account of relevant exemptions to the financial services promotions offence), so long as they are compliant with their fraudulent advertising duties in doing so.

A9.38 We acknowledge that fraudulent advertising judgements regarding the financial promotions offence are made in a different context from content judgements regarding this offence for UGC and search content.[19] However, it remains true that FSMA is highly complex, and that making a fraudulent advertising judgement about the financial promotions offence would likely require technical expertise which it is not proportionate to expect service providers to have access to in-house. However, providers remain free to moderate according to policies which do not take account of relevant exemptions, so long as in doing so they are compliant with their fraudulent advertising duties.

A9.39 Equally, our approach should not dissuade service providers who do have access to sufficient technical expertise from making (or continuing to make) comprehensive fraudulent advertising judgements about all aspects of the financial services offence. Providers wishing to make reasonable inferences about authorisation status or relevant exemptions from the need to be authorised may wish to appoint legal counsel to access such expertise. They may also wish to consult extensive guidance published by the FCA on these matters in the form of the Perimeter Guidance Manual (PERG), part of the FCA Handbook.[20]

A9.40 We consider that, were Ofcom to publish further guidance in addition to that already published in PERG, this would risk further confusion for providers. We therefore propose to

---

[16] Except where an individual at the service provider who is reviewing the opinion is aware of evidence to the contrary, which is unavailable to the FCA or PRA.

[17] The FCA Warning List is a list of unauthorised firms that the FCA has identified may be providing services or products in breach of one or more offences relating to the offences in section 40 of the Act (also the priority offences originating in FSMA as laid out in Schedule 7 to the Act). See FCA, 2026. FCA Warning List of unauthorised firms. [accessed 16 May 2026].

[18] Ofcom, November 2023 Consultation. Volume 5, pp. 37 and 38.

[19] Paid-for advertisements are promotional by nature, and providers typically have more information about the individual or firm placing an advertisement compared to UGC.

[20] See in particular PERG Chapter 8 on financial promotions (8.9 for approvals and 8.11-17 on exemptions). Source: FCA, 2026. Perimeter Guidance (PERG). [accessed 14 May 2026]. See also information included as part of the FCA's Finalised Guidance FG24/1. Source: FCA, 2024. FG24/1: Finalised guidance on financial promotions on social media. [accessed 14 May 2026].

direct providers to the FCA's existing guidance on these offences, rather than providing detailed information on the matters ourselves.

A9.41 Nonetheless, we recognise that there is a high risk of harm from advertisements amounting to the financial promotions offence. As such, we are proposing that financial services verification should be included in our proposed Account Checks and Actions measure (Volume 3, Section 2).

A9.42 This proposed measure recommends that providers apply a financial services verification policy designed to prevent individuals and firms who are not legally entitled to advertise financial services to UK users from doing so on their services. In line with our proposed measure, any policy should incorporate checks for FCA authorisation using the FCA's Financial Services Register, and checks for appearance on the Warning List as a minimum. Providers wishing to incorporate further checks to acknowledge relevant exemptions or approvals from an authorised firm would be able to do so by specifying this in their policy and applying verification checks designed to prevent the advertising of fraudulent financial services.

Articles for use in frauds

A9.43 We propose to add the following to our box of examples of content which may amount to an offence of making or supplying articles for use in fraud: "an advertisement offering to sell an online advertising account, outside of formal business restructuring or provider-approved processes." We do so in recognition of evidence that bad actors are trading accounts with the ability to post paid-for advertisements for profit, enabling other bad actors to post fraudulent advertisements more easily.[21]

Misleading statements and impressions

A9.44 We propose to adapt the explanation we use in the ICJG, without any substantive changes. We explain in the Fraudulent Advertising Judgements Annex how it relates to advertisements.

Cross-cutting proposals

Reasonably available information: Information about the destination of an advert and use of URL-scanning technology

A9.45 On both Category 1 services and Category 2A services, we consider that information about the destination of an advertisement (including landing pages within a single interaction and, in more limited scenarios, other linked webpages) may constitute relevant and reasonably available information, depending on the circumstances.

A9.46 We propose to add outputs from URL-scanning tools and services to the Fraudulent Advertising Judgements Annex's list of 'reasonably available information' for fraud by false representation and misleading statements and impressions about investments, while also recognising that such information will not always be available to the service provider. We discuss this under the heading 'Reasonably Available Information' in the Fraudulent Advertising Judgements Annex (see Annex 11) , and note there that where we consider information from landing pages to be relevant to fraudulent advertising judgements, we

[21] Tech Transparency Project, 2022. Facebook Black Market for Ad Accounts Raises New Scam, Election Interference Fears. [accessed 7 May 2026].

have indicated as such in a grey box outlining types of reasonably available information that should be considered[22].

A9.47 For paid-for advertisements on Category 2A (i.e. search) services, the definition of a paid-for advertisement which may be encountered in or via search results of the service, includes landing pages[23] of the search advertisement, where encountered as a result of a single interaction with the advertisement in search results (such as by clicking on it). On Category 1 (i.e. user-to-user) services, the definition of paid-for advertisements encountered by means of the service include the content of the advertisement itself as well as the associated URL, but not any landing pages. Nevertheless, in some circumstances we consider that the landing page of an advertisement could be particularly relevant when making a content judgement about an advert on a user-to-user service. Relevant examples include:

- if a service provider is assessing whether the landing page matches the content of the advertisement (or is a cloned website impersonating something shown in the advert); or
- when a service provider is assessing whether the landing page has been altered after the advert was submitted or displayed; or
- if a link to a landing page or another linked webpage on that site has been included in a report to the provider about a suspected fraudulent advertisement.

Relevance to impersonation, cloned website and "cloaking" of advertisement destinations

A9.48 We have included these examples because of evidence about impersonation, cloned websites[24] and concerns and evidence about a practice known as "cloaking" to conceal the destination or landing page to which an advertisement leads. Bad actors can use cloaking mechanisms to show different versions of a landing page depending on who – or what system – is accessing it. A fraudster can use cloaking to present a service's review system with a legitimate-looking landing page, while a user may be directed to a different landing page containing fraudulent content. This allows fraudsters to conceal the real landing page from the service's scanning and review systems, thereby evading detection of fraudulent content.[25]

---

[22] As noted in paragraph 1.60 of the ICJG, we recognise that service providers may have access to further information beyond what is specified in examples in this guidance. Where such information is relevant to content judgements as set out in this guidance, service providers may and should consider this information, but only so long as it is processed lawfully, including in particular in line with data protection laws.

[23] Many paid-for advertisements include a 'click-through' that opens a destination such as an external webpage. We refer to this as the 'landing page'.

[24] Website cloning is where bad actors impersonate a legitimate organisation or business by recreating its website, often with no or minimal differences and using a near-identical URL. In doing so, they hope to encourage users to input information, including financial information which can then either sold on or else used to perpetuate further fraud.

[25] Cloaking is a practice whereby fraudsters conceal the destination or landing page to which an advertisement leads. Landing page cloaking can take different forms. One form involves changing a legitimate URL destination to a fraudulent or malicious after an advertisement has been reviewed and gone live. Another form involves tailoring landing page content for users (human or machine) based on visitor characteristics. This allows for legitimate content to be displayed to services, while displaying fraudulent or malicious content to other users. For evidence on the uses of cloaking and impersonation, see Volume 1, Section 4, 'Causes and impacts of fraudulent advertising', sub-section, 'Content risky characteristics'.

A9.49 We are aware of the use of automated URL-scanning technology among many providers of category 1 services.[26] Such technology may be able to provide valuable, simple indicators of fraudulent activity, which may be especially useful for making fraudulent advertising judgements about false representations and misleading statements and impressions about investments.

A9.50 However, there are notable limitations to the use of such automated technology:

- Fraudsters' use of camouflaging techniques such as cloaking, as stated by the Advertising Standards Authority (ASA) in its response to our 2024 Call for Evidence.[27]
- Risk of false flag (i.e. mistaking a flag for a legitimate URL that has not been reviewed and rectified at the time a content judgement is being made).
- Risk of flags relating to matters which are not pertinent to non-priority fraud offences (e.g. sale of counterfeit goods without any false representation being made).

A9.51 Where these tools are relied upon, providers should undertake suitable due diligence and data assurance processes. This includes a service provider taking reasonable steps to mitigate against the risk of incorrect detection outcomes. Service providers should also ensure that, where outputs suggest a URL destination is associated with fraud, the type of fraud concerned is relevant to the offences set out in section 40 (for example, an unregulated investment or consumer scam).

A9.52 We are also aware that URL-checking services are available (often accessed through websites), which may be used to obtain similar information about a URL as those provided by automated URL-checking technology used by a service provider. In the ICJG, we referred to the use of such services as a means of mitigating the risks posed when accessing links in potentially fraudulent UGC. To rely on outputs from URL-checking services as reasonably available information when making a fraudulent advertising judgement, the same best practice considerations apply as set out in paragraph A9.51 to A9.52[28]

References to Consumer Protection from Unfair Trading Regulations 2008 and regulation by the Advertising Standards Authority (ASA)

A9.53 Since we published the ICJG, the Consumer Protection from Unfair Trading Regulations 2008, which we referenced in paragraph 6.8 of the ICJG introduction, have been superseded by obligations in the Digital Markets, Competition and Consumers Act 2024. These obligations came into effect regarding online advertisements from 6 April 2025.

A9.54 As such, we propose to update our references to the 2008 Regulations to reflect this, both in the ICJG and the draft Fraudulent Advertising Judgements Annex. We also propose to make consequential amends to the ICJG in paragraph 6.3.

A9.55 We also propose to include additional text which recognises the existence of a parallel regime for misleading advertising, run by the ASA with technical elements of misleading financial advertising delegated to the FCA. We state in the draft Fraudulent Advertising Judgements Annex that "[a]dvertisements which are misleading but not fraudulent are not

[26] Automated URL-scanning technology allows click-through destinations included in advertising content to be scanned for potential threats, such as malware, phishing, or fraudulent activity such as the sale of counterfeit products or investment scams.
[27] ASA response to 2024 Call for Evidence, p.4.
[28] In applying those best practice considerations, providers should bear in mind that the transparency of the systems and data employed by URL checking websites may vary.

within scope of the additional duties regarding fraudulent advertising" but such advertisements may nevertheless be subject to separate action by the ASA.[29]

Use of ICJG illegal content judgement guidance

A9.56 To promote simplicity and accessibility, we have used the ICJG fraud chapter as a basis for the Fraudulent Advertising Judgements Annex. We propose to append a new text on how to make fraudulent advertising judgements to the ICJG, as we believe this is simplest and most accessible choice.

A9.57 At A3.4 to A3.5 in our Fraudulent Advertising Judgements Annex, we explain that providers should consult Chapter 1 of the ICJG when making fraudulent advertising judgements, because much of what is set out there will be relevant. We list the parts of Chapter 1 which we do not consider to be relevant to these judgements at A3.4, and we also make clear that when referring to Chapter 1 of the ICJG, references to 'illegal content' and 'illegal content judgements' should be read as references to 'fraudulent advertising' and 'fraudulent advertising judgements' respectively.

A9.58 We recognise that both fraudulent advertising judgements and illegal content judgements involve consideration of the same offences, using the same threshold of reasonable grounds to infer, and that both require consideration of reasonably available information.

Minor consequential amendments to Chapter 1 of the ICJG (Introduction)

A9.59 We are also proposing to make minor consequential amendments to Chapter 1 of the ICJG (Introduction). Broadly these relate to amending the explanation of the scope of the ICJG to make it clear that it covers fraudulent advertising judgements and refers to the Fraudulent Advertising Judgements Annex. These proposed changes to Chapter 1 of the ICJG appear in markup at Annex 10. We will also update the contents page of the ICJG accordingly.

[29] The ASA's Committees of Advertising Practice (CAP) non-broadcast code has rules that cover non-broadcast advertising (including online advertising). It specifies standards for accuracy and honesty that businesses must stick to, including specific conditions, such as advertising to children and causing offence. The rules are enforced by the ASA. For more information see: ASA, 2014. The CAP Code. [accessed 14 May 2026]

Fraudulent Advertising Codes Consultation

Annex 10: Draft amendments to the Illegal Content Judgements Guidance – Chapter 1

Proposed changes to Chapter 1 of the ICJG appear in markup in this annex

Consultation

Published 10 July 2026
Closing date for responses: 02 October 2026

Introduction

About this document

1.1 This document is Ofcom's Illegal Content Judgements Guidance ('**ICJG**') for the purposes of section 192 of the Online Safety Act 2023 ('the **'Act'**). The Act introduces a new legal concept of 'illegal content', which is used in the risk assessment duties and safety duties for service providers.[1] ~~It may also be relevant for Category 1 services~~[2]. The guidance is intended to support part 3 service providers[3] in understanding their regulatory obligations when making judgements about whether content is illegal content for the purposes of any of these duties (**'illegal content judgements'**). These concepts are explored below in paragraphs 1.14-20 of this guidance. Under section 192, Ofcom must also produce guidance on judgements by providers of Category 1 and 2A services about whether content is a fraudulent advertisement.[4] In addition to making illegal content judgements regarding user-to-user or search content, these providers also need to make additional content judgements regarding paid-for advertising content ('fraudulent advertising judgements').[5] Ofcom's guidance on fraudulent advertising judgements is contained in Annex 3.

1.2 Section 192 of the Act sets out the approach to be taken where either a system or process operated or used by a service provider to comply with the Act, or a risk assessment, involves a judgement by the service provider about whether content is illegal content (or fraudulent advertising. The Act requires that service providers make such judgements based on a reasonable inference. The Act states that content will be illegal content where there are reasonable grounds to infer that:

the conduct element of a relevant offence is present or satisfied;
the state of mind element of that same offence is present or satisfied; *and*
there are no reasonable grounds to infer that a relevant defence is present or satisfied.

1.3 This threshold of 'reasonable grounds to infer' is lower than the criminal threshold ('beyond reasonable doubt') that is applied in the UK's criminal justice system.

1.4 When making illegal content judgements, service providers ~~have a duty~~ must have regard to the right to freedom of expression within the law. However, there is nothing in the Act that requires service providers to make illegal content judgements, so long as the application of

[1] We use the term 'service provider' interchangeably with 'providers of regulated user-to-user services and regulated search services.'

[2] ~~There are additional duties in relation to Category 1 service providers only which relate to (1) protecting news publisher content and (2) fraudulent adverts. We will be consulting on the requirements of the Act for Category 1 service providers at a later date. If we need to amend this guidance we will consult on the proposed amendments if necessary.~~

[3] Part 3 service providers are regulated user-to-user and search service providers under Part 3 of the Online Safety Act

[4] This requirement is set out in section 193 of the Act.

[5] We note that section 193(2)(a) of the Act treats judgements about whether content is a fraudulent advertisement as a kind of 'illegal content judgement'. For the purpose of this guidance, we use the term 'illegal content judgement' in a more limited sense, to refer to a judgement about whether content is 'illegal content' for the purpose of providers' compliance with the illegal content safety duties in Part 3 Chapters 2 and 3 of the Act. This is distinct from a judgement about whether paid-for advertising content is a 'fraudulent advertisement' for the purpose of Category 1 and 2A providers fraudulent advertising duties under Part 3 Chapter 5 of the Act, which we refer to as a 'fraudulent advertising judgement'.

that service provider's own terms and conditions is sufficient to secure compliance with the duties in the Act in other ways. For example, if the service provider's own terms and conditions of use prohibit content that is wider than the definition of illegal content under the Act, then the service provider would be considered to have fulfilled its legal duties regarding takedown so long as it applied these terms and conditions properly. Ofcom does not have a power under the Act to compel providers to carry content they do not wish to carry. In practice, this means that services may continue to operate with regard to Terms and Conditions which prohibit *more* content than is covered in this Guidance, though they will not be compliant if their Terms and Conditions capture *less*. However, when making illegal content judgements, we encourage providers to consider carefully the impacts of their choices on users' opportunities to express themselves.

1.5 Ofcom must produce guidance on the matters dealt with in section 192. This document, the Illegal Content Judgements Guidance (the **Guidance**), including the guidance on fraudulent advertising judgements contained in Annex 3, fulfil that obligation.

1.6 As a public authority, Ofcom must carry out our functions compatibly with the Human Rights Act 1998, including the rights to freedom of expression and respect for private and family life ('**privacy'**). Any interference with the right to freedom of expression must be prescribed by law, pursue a legitimate aim and be necessary in a democratic society. Any interference with the right to privacy must be in accordance with the law, pursue a legitimate aim and be necessary in a democratic society. In order to be 'necessary', the restriction must correspond to a pressing social need, and it must be proportionate to the legitimate aim pursued.

1.7 Ofcom has had careful regard to these rights in producing this guidance. Both the definition of illegal content and the requirement for Ofcom to prepare this guidance are set out in the Act and pursue the aims of the prevention of crime, the protection of health and morals, and the protection of the rights of others.

1.8 The definition of illegal content in the Act is based on UK criminal offences, which are complex, nuanced and not always fully defined in legislation. They often require consideration of people's state of mind; for example their 'intent'. As such, while we have tried to set out clear signposts and an easy-to-navigate approach, there are limits to how much we can simplify the language and concepts in this document. In addition to the information given in this guidance, service providers should refer to Ofcom's Register of Risks for further detail on how offences may manifest online.

1.9 It is also necessary to discuss topics in this document which some may find very upsetting. We have tried to treat such topics sensitively, and note where a proper reflection of the law requires us to use language which may be seen as controversial or problematic.

1.10 The contents of this document represent an effort by Ofcom to provide service providers with a sound basis on which to make illegal content judgements and fraudulent advertising judgements, rather than an attempt to anticipate every circumstance which may arise during moderation. Context is crucial to determining the nature of content.

1.11 UK criminal law changes and develops over time. This guidance is not a substitute for any regulation or law and is not legal advice. Where required, service providers should seek their own independent advice to enable them to understand and comply with their duties under the Act.

Structure and formatting

1.12 This document is structured as follows:

a) Introductory information, Chapter 1; setting out legal background, key concepts and principles which apply to all illegal content judgements.

b) Offence-specific chapters, Chapters 2-16, giving overviews of offences and guidance as to how to make illegal content judgements in relation to them. N.B. offences are grouped by type as appropriate; see paragraphs 1.71 to 1.76 for more information on how to use this section.

c) Legal annexes 1 and 2; setting out more detailed legal information to support the guidance given in offence-specific chapters.

d) Annex 3: Guidance on fraudulent advertising judgements; this sets out legal background, key concepts and principles which apply to fraudulent advertising judgements.

1.13 Where we have used words with a special technical meaning, these are highlighted in '**bold**' and represented in quotation marks in the first instance for ease of comprehension. Summaries or names of offences are also presented in **bold** for ease of identification. Essential messages regarding process and approach are marked with an underline.

Services' duties regarding illegal content

1.14 The Act creates many new legal duties for service providers. These include risk assessment and safety duties in relation to illegal content[6], content reporting, complaints procedures and freedom of expression and privacy.

1.15 This guidance should be used by service providers in all circumstances when they are required to make a judgement on whether content is illegal in order to fulfil their duties under the Act.

1.16 Such judgements may be made in order to conduct illegal content risk assessments (section 9 for user-to user ('**U2U'**) Services and section 26 for search services) ('**illegal content risk assessment duty**') and to implement measures to comply with their safety duties regarding illegal content (section 10 for user-to-user services and section 27 for search services) ('**illegal content safety duty**'). Regarding Category 1 services, judgements around illegality may need to be made in relation to their duties to protect news publisher content and duties in relation to fraudulent advertising. Together, these are the '**illegal content duties**'.

1.17 Within the illegal content duties there are a number of specific duties. As part of the illegal content safety duty at section 10(3)(b) of the Act, there is a duty for a user-to-user service provider to operate the service using proportionate systems and processes designed to "swiftly take down" any illegal content where it is alerted to the presence of such content or is aware of its presence in any other way (the '**takedown duty**'). Search services have a duty to minimise the risk of users encountering search content that is illegal content (section 27(3) of the Act).

[6] Illegal content is defined in the Act as 'content which amounts to a relevant offence.' For more information on relevant offences and illegal content see paragraphs 1.24-34 of this guidance.

1.18 When service providers conduct risk assessments and implement measures in accordance with their safety and other duties, they are likely to be dealing with content in bulk, as opposed to making an assessment on an individual piece of content. Service providers should anticipate that some of the content they hold is likely to be illegal content, but can do this on a probabilistic basis. For example, a service provider which has a livestreaming function should recognise the risk that the function may be used to create child abuse-related illegal content, even if they cannot identify a specific livestream which amounts to such content. Service providers are likely to find this guidance helpful in understanding different types of illegal content which, in turn, will help inform their risk assessment.

1.19 To make decisions for the purposes of the takedown duty or determining what search content is illegal content, service providers will need to take decisions about specific pieces of content. It is here that this guidance will be particularly useful.

1.20 We recognise that service providers are likely to make content moderation judgements in accordance with the laws of each country in which they operate. This guidance is not intended to override or supersede existing moderation practices, where these practices already meet the duties set out in the Act.

Freedom of expression and privacy

1.21 It remains open to service providers as a commercial matter (and in the exercise of their own right to freedom of expression), to prohibit and take down content that is not or might not be illegal content, so long as they abide by the Act. For example, some service providers use their terms and conditions to prohibit sexual content or nudity of any kind on their services. It is open to them to do this, notwithstanding that such sexual content might not be illegal content. This guidance is intended to help service providers identify when operating in accordance with their duties pursuant to the Act *requires* them to take the content down.

1.22 When assessing conformity with the illegal content duties, Ofcom may consider whether a service provider's illegal content judgements follow the approaches set out in section 192 of the Act and this guidance.

1.23 Service providers should make illegal content judgements in accordance with their duties relating to freedom of expression and protection of privacy, as set out in sections 22 and 33 of the Act. These duties state that, when deciding on and implementing safety measures and policies, service providers should have particular regard to the importance of protecting users' right to freedom of expression within the law, and to the importance of protecting users from the breach of any statutory provision or rule of law concerning privacy. Privacy law includes, but is not limited to, data protection law, which is set out in the UK GDPR and the Data Protection Act 2018. The Privacy and Electronic Communications Regulations (PECR) may also be relevant. These are enforced by the Information Commissioner's Office (the ICO). The ICO has a range of guidance on data protection and the PECR which service providers may wish to consult.

Illegal content

Box 1: The Act's definitions of content, search content, illegal content, and relevant offences

Content: anything communicated by means of an internet service, whether publicly or privately, including written material or messages, oral communications, photographs, videos, visual images, music and data of any description.

Search content: content that may be encountered in or via search results of a search service, *except*: paid-for advertisements, content on the website of a recognised news publisher, or content that reproduces or links to content originally published by a recognised news publisher.

Illegal content: regulated user-generated content which amounts to a relevant offence. Content is illegal content where there are reasonable grounds to infer that: a) the conduct element of a relevant offence is present or satisfied; b) the state of mind element of that same offence is present or satisfied; *and* there are no reasonable grounds to infer that a relevant defence is present or satisfied.

Relevant offences: comprise the priority offences set out in schedules 5-7 of the Act, as well as any non-priority or 'other' offence within subsection (5) of section 59 of the Act.

1.24 Content is defined as "anything that is communicated by means of an internet service, whether publicly or privately".[7] This includes written material or messages, photographs, videos, visual images, oral communication, music and data of any description. Comments, titles and descriptions are also considered to be 'content', as are livestreaming videos or audio, and hyperlinks.

1.25 Search content is content which may be encountered in or via search results of a search service, following a 'one click away' principle, *except* where the content is a paid-for advertisement, content on a website of a news publisher, or content which reproduces an article or video/audio originally published by a news publisher (or links to these).

1.26 Illegal content is defined in the Act as "content which amounts to a relevant offence". That is, content that amounts to priority offences (see paragraph 1.28 to 31) or any 'other' offences where the victim is an individual and the offence does not touch on trading standards or intellectual property rights (see paragraphs 1.32 to 1.34). It is the content itself which must amount to the offence. Content which just depicts an offence (for example, a video of a violent attack on someone) is not necessarily illegal content, although service providers may need to consider carefully whether, for example, it encourages terrorism.

1.27 Content 'amounts to' a relevant offence if:

a) the use of the words, images, speech or sounds amounts to a relevant offence,

b) the possession, viewing or accessing of the content constitutes a relevant offence, or

c) the publication or dissemination of the content constitutes a relevant offence.

However, to determine when content 'amounts to' a relevant offence, a service provider must make an illegal content judgement.

[7] Section 237 of the Act.

Figure 1.1: How 'illegal content' relates to 'relevant offences'[8]

Priority offences

1.28 Relevant offences comprise two types: priority offences, and 'other' offences. The priority offences are listed in schedules 5, 6 and 7 of the Act and cover terrorism, child sexual exploitation and abuse (CSEA), and a number of other areas. More details on priority offences, including the elements of the offence that must be present, can be found in the Legal Annex companying this guidance.

1.29 Within priority offences, there is an additional group of offences which are referred to in UK law as 'inchoate offences.'[9] Inchoate offences happen when someone is involved in an offence, without committing it themself. For example, a person may 'assist' in a robbery if they drive the getaway car. They did not carry out the offence, but they were involved in it.

1.30 There is considerable overlap between the inchoate offences. The inchoate offences are:

a) Conspiring (with one or more others) to commit an offence. A conspiracy is an agreement between two or more people to commit an intended offence (or one or more intended offences).[10]

b) Encouraging (someone) to commit an offence. This overlaps with inciting, counselling or procuring and aiding and abetting the commission of a priority offence.

[8] Priority offences are named in the Act in schedules 5, 6 and 7. For details on 'other' offences, see paragraphs 1.32-4 below.
[9] Inchoate offences are found in schedule 5(4), schedule 6(9 and 13), and schedule 7(39) of the Act.
[10] It should be noted that there is no offence of 'attempting to conspire', so a person trying and failing to engage in a conspiracy will not thereby generate any illegal content.

c) Assisting (someone) to commit a priority offence. This overlaps with aiding and abetting the commission of a priority offence.

d) In Scots law, being involved art and part in committing a priority offence. A person is involved 'art and part' in the commission of an offence if they knowingly engage with someone else in pursuit of a common purpose to commit the offence. This overlaps with conspiring and assisting but can be broader than either.

e) Attempting to commit an offence. We are not aware of any circumstances in which this could take place online, and so we do not talk about it further in this guidance.

1.31 Where we believe it is particularly important that conspiring, encouraging, assisting and 'art and part' offences are considered alongside the other priority offences, we have indicated this in the appropriate section in Chapters 2 to 16. The inchoate offences will be particularly important to consider in relation to those priority offences which cannot themselves be committed online.

Relevant non-priority offences ('other' offences)

1.32 'Other' offences are offences that are (1) not priority offences but where (2) the victim or intended victim of the offence is an individual or individuals. For this reason, we refer to them in the rest of this document as **'relevant non-priority offences'**.

1.33 In recognition of the quantity and complexity of offences which could be included within the scope of the definition of 'other' offences, Ofcom has chosen to provide specific guidance on 'other' offences where they appear to us particularly likely to arise online in the form of content, and do not overlap substantially with priority offences. These offences comprise the following:

a) *Epilepsy trolling offence*; that is, the offence of sending a flashing image with the intention that it would be seen by a person with epilepsy or where it was reasonably foreseeable that this would be the case. See section 183 of the Act.

b) '*Cyberflashing' offence*; that is, the offence of sending or giving a photograph or video of the genitals with the intent of causing alarm, distress or humiliation, or for the purpose of sexual gratification on the behalf of the sender (with recklessness as to whether alarm, distress or humiliation could be caused). See section 187 of the Act.

c) *Self-harm offence*; that is, the offence of assisting or encouraging 'serious' acts of self harm. See section 184 of the Act.

d) *False communications offence*; that is, sending a message which conveys knowingly false information with the intent of causing non-trivial psychological or physical harm to the likely audience (without reasonable excuse for sending). See section 179 of the Act.

e) *Section 127(1) offence;* we have focused on a particular aspect of this offence, to capture content depicting torture or extreme cruelty in such a way as to be obscene.

1.34 Chapter 16 of the ICJG deals with how a service provider should consider content which may amount to a relevant non-priority offence which is not specifically covered in this guidance.

Jurisdictional considerations

1.35 For the purposes of determining whether content is illegal, the Act states that it is not relevant "whether or not anything done in relation to the content takes place in any part of the United Kingdom."[11] This means that, for example:

a) It does not matter whether or not the user uploading the content, the service hosting the content or the person accessing the content are in the United Kingdom. A person outside the United Kingdom using a service outside the United Kingdom to harass a person outside the United Kingdom may still generate illegal content for the purposes of the Act.

b) Content can amount to a Scottish priority offence even if the user posting the content, the service provider itself and the user viewing the content were in England.

1.36 However, where the offence concerned involves an element of offline behaviour, service providers may still need to consider location. Where this is the case, we explain how this should be done in the guidance. If the guidance is silent on this point, location should be taken to be not relevant.

1.37 Due to the significant overlap between laws in the United Kingdom's three legal jurisdictions, England and Wales, Scotland, and Northern Ireland, the practical impact of jurisdictional differences is limited. There are, however, isolated cases where a law in one part of the United Kingdom is different from the other jurisdictions. Where this is the case, we have set out an appropriate approach to be taken which takes account of differences and service providers should consult the appropriate section in Chapters 1 to 16 of this guidance.

Facilitation of relevant offences

1.38 Under section 10(2)(b) of the Act, U2U service providers are required to take or use proportionate measures to ensure that the design or operation of their service mitigates and manages the risk of the service being used for the commission or facilitation of a priority offence. Further information on services' duties in relation to facilitation of offences is set out in the Service Risk Assessment Guidance and evidence of such facilitation has been included in the Register of Risks.

1.39 It is possible for specific items of content to facilitate the commission of an offence without it amounting to illegal content (by reference to the legal definitions explained above). For example, an adult talking to a child online may be preparing or intending to commit an offence, but not yet have done so. The guidance in this document relates to illegal content only and does not touch on content which would amount to the facilitation of an offence. However, if an illegal content judgement as set out in this document does not result in the content in question being taken down, service providers should also consider whether the content in question facilitates an offence and whether the design and operation of their services is effectively mitigating the risk of such content.

[11] Section 59(11). See also the Explanatory Notes to the Act, which provide in relation to section 59 of the Act: "Under subsection (11), content does not need to be generated, uploaded or accessed (or have anything else done in relation to it) in any part of the United Kingdom to amount to an offence under this provision. This is the case regardless of whether the criminal law would require any relevant action to take place in the United Kingdom (or a particular part of it)".

Illegal content judgements

Reasonable grounds to infer

Background

1.40 In UK criminal law, all offences comprise three elements, each of which needs to be considered in relation to a particular person, the 'defendant' (usually the user who has done something in relation to the content):

a) the action or conduct element of the offence (legally known as the 'actus reus');

b) the state of mind or mental element of the offence; that is, the state of mind required for the offence (legally known as the 'mens rea')[12]; and

c) any relevant defences. In this context, if a defence could be reasonably inferred to be present, the content is not illegal content.

1.41 The three elements of each priority offence are set out in the legal annex accompanying this guidance.

1.42 Content will amount to illegal content for the purposes of the Act when there are reasonable grounds to infer that the conduct and state of mind elements are present and satisfied, unless there are reasonable grounds to infer that a defence is present or satisfied:

1.43 Reasonable grounds to infer is not a criminal threshold, and there are no criminal implications for the user if their content is judged to be illegal content against this threshold. The service is not obliged to report illegal content to law enforcement except where the content in question is subject to requirements to report CSEA content to the NCA, as set out in section 67 of the Act.

1.44 We are aware that some service providers may choose to maintain bilateral relationships with law enforcement or internal processes which allow them to escalate content to law enforcement where appropriate. Nothing within this guidance should be taken as discouragement to maintain such relationships and internal processes.

Establishing reasonable grounds to infer

1.45 If making an illegal content judgement, service providers should ensure that they:

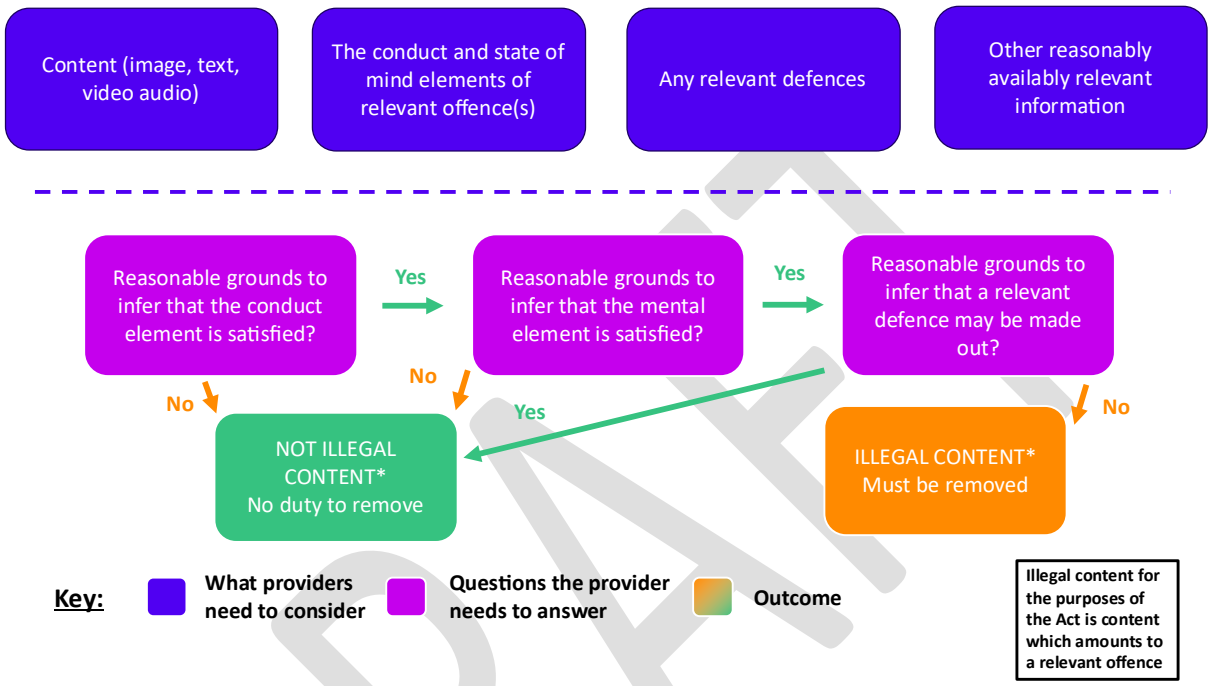
a) Possess sufficient understanding of UK law (see the legal annex accompanying this guidance); and

b) Take into account all relevant 'reasonably available information' (see paragraphs 1.60 to 1.65, below)

1.46 Figure 1.2 sets out how service providers may establish whether reasonable grounds to infer that content is illegal exist in any case. However, when making illegal content judgements service providers should consult the appropriate chapter in this guidance for offence-specific information including a summary of legal and contextual considerations.

[12] Mens rea requirements vary across offences and can include: acting with intent, acting recklessly, acting dishonestly, or acting with knowledge. The mens rea requirement of all priority offences are set out in the legal annex accompanying this guidance.

Figure 1.2: Overview of reasonable grounds to infer



1.47 Chapters 2 to 16 explain (where possible) how each priority offence and select non-priority offences may manifest in illegal content, the action and mental elements that must be present in the content, the defences that must not be present, and the information a service should consider in order to make such a judgement.

Attributing conduct and state of mind to individuals

1.48 The Act requires service providers to make a judgement about conduct, state of mind and defences. This means it is necessary first to identify a person in relation to whom these things are being assessed. The person is someone whose actions *in relation to the content* may involve a criminal offence. This will most often be the person posting, uploading or sharing the content, but this may not always necessarily be the case. For example, the offence of collecting information likely to be of use to a terrorist can be committed in several ways, including by viewing or otherwise accessing content by means of the internet. Usually there will be no need for service providers to consider this nuance, but if the user uploading the content had a defence for doing so, the same might not be true of users viewing or accessing it and so the content may still be illegal content.

1.49 Content is not illegal content merely because it depicts a crime. For example, an item of content may depict one person violently attacking another. The service provider does not need to consider whether the attack itself is a criminal offence and as such it does not need to consider the conduct, state of mind or defences available to the person depicted in the content as carrying out the attack. Rather, it needs to consider whether there are reasonable grounds to infer that the person who has posted, uploaded or shared the piece of content has committed an offence by doing so.

1.50 Service providers do not necessarily need to know the identity of the user to draw this inference. For example, if a user says their account has been hacked, that does not necessarily mean that content posted is not illegal content, since the person who hacked it would be the user posting the content.

Conduct and state of mind when content has been posted by a bot

1.51 Bot is an umbrella term that refers to a software application or automated tool that has been programmed by a person to carry out a specific or predefined task without any human intervention. Bots are often employed on services to post content at scale without the need for repeated human intervention. In many cases bots are used for benign purposes; for example, a bot may be used to post automated weather forecasts, to automatically 'cross-post' content across multiple services operated by the same user, or to respond to customer posts on a brand's social media profile speedily out of working hours. However, bots may also be used to spread spam and malicious content, including misinformation and phishing attempts.

1.52 Bots are not alive, so cannot commit offences. However, section 192 of the Act states that, where content has been posted by a bot, inferences about the conduct and the presence of the mental element, and any defences, should be made by considering:

a) the actual person controlling the bot or tool, where this is known to the service; or

b) the person who may be assumed to be controlling the bot, where the actual identity of the person is not known.

1.53 Where we believe that bots play a notable role in the generation of illegal content, we note this in our in-depth guidance in Chapters 2 to 16.

Inferring state of mind

1.54 As a matter of UK law, almost all the priority offences have a 'mental element' or state of mind requirement, which must be satisfied in order for reasonable grounds to infer to exist. These are matters of UK law, and it is not open to Ofcom to change them or put them to one side. The four most common types of mental element relating to the priority offences involve:

a) Acting with intent (for example, intent to cause a person harassment, alarm or distress, or intent to encourage others to commit, prepare or instigate acts of terrorism);

b) Acting recklessly (for example, being reckless as to whether a statement made about a financial promotion is false or misleading). Being reckless means the person recognised the risks of an action but went forward with an action or behaviour anyway. For English, Welsh and Northern Irish offences, recklessness is usually subjective, for example, the test is not whether a reasonable or typical person would have recognised the risk, but whether the actual defendant in question did. For Scottish offences recklessness is usually objective (for example, based on what a reasonable person would have realised);

c) Acting dishonestly (i.e. what was the person's actual state of knowledge or belief relating to the facts and was his conduct dishonest by the standards of ordinary decent people? A person's beliefs as to whether the conduct would be seen as dishonest by others is not relevant.) It is not dishonest to make a mistake, or to make a joke;

d) Acting with knowledge (for example, acting with knowledge or suspicion that a substance being offered for sale is a psychoactive substance). What a person has to know, and the degree to which they must know it, varies from offence to offence.

1.55 It is not possible to give substantial guidance on these concepts in the abstract. What amounts to reasonable grounds to infer will differ from offence to offence and will often be dependent on the context of the content. We recognise that in some cases, particularly where there may be many reasons for a person to do as they have done, it will likely never be possible to reach firm conclusions about a poster's state of mind. However, the Act does not require proof to the criminal standard, and therefore neither will Ofcom when assessing a provider's compliance. When inferring state of mind as part of an illegal content judgement, service providers should rather be seeking to reach a *reasonable inference* based on the information available to them and the circumstances they are aware of, having paid regard to this guidance.

Inferring state of mind when content has been shared, forwarded or reposted

1.56 In cases where the service provider is aware that a piece of content has been shared, forwarded or reposted from another user, either with or without alteration or addition, the reforwarded, reshared or reposted content will be treated as a new piece of content for the purpose of an illegal content judgement. The service provider should make inferences about the state of mind of the user that has re-shared the content, rather than the original author of the post. For some types of offences, particularly extreme pornography and child sexual abuse material (CSAM), the content will remain illegal content. For other priority offences, however, the illegality of the content in each new iteration will depend upon the likely state of mind of the person sharing, forwarding or reposting it.

The importance of context

1.57 We acknowledge that it is likely to be necessary for service providers to make illegal content judgements at scale, without any powers to collect and assess *all* relevant information and without a complete understanding of the contextual circumstances pertinent to each individual piece of content.

1.58 Context is extremely important to a proper understanding of many offences and can be the difference between the reasonable grounds to infer threshold being met or not. For example, out of context, a message or other post containing threatening or abusive language may amount to an offence under section 38 of the Criminal Justice and Licensing (Scotland) Act 2010. However, there are clear cases where context would suggest that an offence has *not* occurred: for example, if the message was sent jokingly between friends, or if a threat was made sarcastically. To make an illegal content judgement, a service provider must consider this context. We recognise that it is not possible to make correct judgements all the time. Appropriately trained and culturally aware content moderators should be empowered to make sensible judgements using the information they have.

1.59 More information on the contextual factors that should be considered in each case is given in the offence-specific guidance in Chapters 2 to 16.

Reasonably available information

1.60 Illegal content judgements should be made with reference to all information that is both relevant and reasonably available to a service provider. Information should only be considered relevant where it helps to infer the presence or absence of any of the three parts of an offence as outlined at paragraph 1.40. Service providers should only process as much personal data as is necessary (having regard to the principle of data minimisation under the UK GDPR, where applicable[13]). The type of information that is relevant to a content judgement will vary depending on the offence being considered.

1.61 The Act states that two factors are particularly relevant in considering the information that is reasonably available to a service provider:

a) "the size and capacity of the provider"; and

b) "whether a judgement is made by human moderators, by means of automated systems or processes or by means of automated systems or processes together with human moderators."

1.62 In our view, the information available for an average or larger service provider that is relevant to an illegal content judgement is also reasonably available to the smallest services. For the time being, based on the evidence available to us, we have taken a 'technology-agnostic' approach to illegal content judgements.

1.63 Ofcom has assessed the availability of information which we believe is relevant to priority offences on an offence-by-offence basis and, where we believe that this information is reasonably available to a service, we have included this as part of the processes set out in Chapters 2 to 16. Underneath each section of our offence-specific guidance, we include a box setting out the information we consider to be reasonably available for the purposes of making judgments in relation to those offences.

1.64 We recognise that content judgments will sometimes be challenging for providers of search services to make based on the relatively limited information available to them in comparison to providers of U2U services. Our ICJG is intended to be used by all services, but where appropriate in this document, we have noted where illegal content is unlikely to be present on search services, and where it is appropriate for search services to draw upon a reduced set of 'reasonably available information' when making content judgements.

1.65 We recognise that service providers may have access to further information beyond what is specified in this guidance. Where such information is relevant to content judgements as set out in this guidance, service providers may and should consider this information, but only so long as it is processed lawfully, including in particular in line with data protection laws. [14] Service providers may not always need to consult all available information in every instance, if it is possible to make an accurate judgement using less information.

[13] The ICO. Principle (c): Data minimisation. [Accessed 20 September, 2023].

[14] As above, information should be considered relevant only where it can be used to infer the presence or absence of the three criteria which must be satisfied in order for reasonable grounds to infer to exist (see paragraph 1.40, above).

Third party flags or reporting

1.66 A provider is not usually required to accept the opinions of a third party as to whether content is illegal content. Only a judgment of a UK court is binding on it in making this determination. Services may also need to have regard to the decisions of experts when compiling hashed lists of child sexual abuse material (CSAM). In all other cases, it will need to take its own view on the evidence, information and any opinions provided. Where a third party only has suspicion that an offence being committed, this is not sufficient *in itself* to reach the reasonable grounds to infer threshold, and service providers should only consider this as part of a wider assessment of the content's illegality.

1.67 We have made one exception to this principle in the case of offences from the Financial Services Markets Act, where we have decided that it is appropriate to steer services to adopt the opinion of the Financial Conduct Authority (FCA) when making judgments about the illegality of content under these offences. This is because these offences are too complicated for a content moderator reasonably to be expected to understand them.

1.68 If any personal data is provided to a service provider from a third party, service providers will need to ensure they comply with data protection law in relation to it. In particular, where applicable, they must have regard to Article 10 of the UK General Data Protection Regulations (GDPR).

Malicious reporting

1.69 In some cases, the existence or details of a user complaint may help service providers to infer the satisfaction of the conduct or behaviour element of an offence. For example, in the case of harassment, the effect of causing alarm or distress is an element of the offence, and a user report may give grounds to infer this.

1.70 When considering reporting information as part of an illegal content judgement in this way, service providers should have regard to the possibility that the report is malicious. A malicious report is one made with the intention of disrupting another user's ability to use a service to post content. Popular accounts by internet personalities or 'influencers' are particularly likely to attract malicious reports, and commercial incentives to disrupt a competitor's business practices may also be a factor. Malicious reports may also be more closely associated with certain harms areas, such as coercive and controlling behaviour (CCB) and harassment, and service providers should be aware that there is a particularly high risk of malicious reporting from any user has previously had content removed (or other action taken) due to breaching terms of service regarding harassment.

How to use the remainder of this document

1.71 The remainder of this document provides descriptions of the priority offences and the non-priority offences we consider likely to occur online. In each chapter, we have considered the offences in order of the likely ease of making reasonable inferences as to whether content amounts to the offence in question.

1.72 To assist service providers, we have included examples of the types of content that may fall into these offences. However, when a service provider is making an illegal content judgement each piece of content will need to be considered on a case-by-case basis with reference to the state of the mind requirements of the offence and any available defences. Service providers should pay particular attention to definitions given, as everyday words often have specific meanings in a legal context. In cases where definitions do not exist, we expect service providers to take a common-sense approach which makes use of the everyday meaning of the terms concerned. This approach is based on what a jury would need to do in a criminal case if terms used in the offence had no legal definition.

1.73 When they have encountered a specific item of potential illegal content, service providers should in the first instance consider whether the content falls within any of the priority offences, other offences considered in this guidance, or any relevant non-priority offence it has reason to suspect may be engaged (referred to in the Act as 'other offences'). Once content has been identified as illegal content under one 'relevant offence', it has met the threshold for removal and there is no need to go on to consider any more offences.

1.74 We have kept the main body of this document as simple as possible, which means we have kept footnotes and legal references out of the drafting. For legal references, and detailed definitions, service providers should refer to the Legal Annex accompanying this document. This is particularly important where our guidance is dealing with multiple overlapping offence from more than one jurisdiction of the UK. The drafting in our main chapters seeks to simplify this for providers as much as possible and will not necessarily correspond to what a lawyer qualified in the law of any one UK jurisdiction will expect to see.

1.75 As noted above, this guidance should not be regarded as a substitute for any regulation or law and is not legal advice. Where required, service providers should seek their own independent advice to enable them to understand and comply with their duties under the Act.

1.76 We recognise that content judgments will sometimes be challenging for providers of search services to make based on the relatively limited information available to them in comparison to providers of U2U services. Our Guidance is intended to be used by all services, but where appropriate in this document, we have noted where illegal content is unlikely to be present on search services, and where it is appropriate for search services to draw upon a reduced set of 'reasonably available information' when making content judgements.

Fraudulent Advertising Codes Consultation

Annex 11: ICJG Draft Annex 3: Guidance on fraudulent advertising judgements

We propose to add this new annex into the existing Illegal Content Judgements Guidance. As it would become “annex 3”, we have used that numbering for paragraphs in this document.

Consultation

Published 10 July 2026
Closing date for responses: 02 October 2026

A3. Guidance on fraudulent advertising judgements

About this annex

A3.1 Under the Online Safety Act 2023 (the '**Act'**), all in-scope services have duties regarding illegal content and content which is harmful to children. In addition, categorised services (being those that meet the conditions relating to user numbers and functionality set out in the relevant legislation) are subject to further duties concerning user empowerment, transparency reporting, protections for news publisher and journalistic content, and preventing UK users encountering fraudulent advertisements. [1] Duties regarding fraudulent advertising apply to Category 1 and 2A services only.

A3.2 This means that, in addition to making illegal content judgements regarding user-to-user or search content, as set out in Chapters 2-16, providers of Category 1 and 2A services ("providers") also need to make 'fraudulent advertising judgements' regarding paid-for advertising content (in this annex we use the term 'fraudulent advertising judgement' to refer to a judgement about whether paid-for advertising content is a 'fraudulent advertisement' which is distinct from an 'illegal content judgement' which refers to a judgement about whether content is 'illegal content' for the purpose of providers' illegal content safety duties).[2] They will need to do this to determine whether a paid-for advertisement meets the definition of a fraudulent advertisement under the Act.

A3.3 Ofcom must produce guidance on the matters dealt with in section 192 of the Act, including fraudulent advertising judgements.[3] This annex is intended to fulfil this requirement.

A3.4 Chapter 1 of the Illegal Content Judgements Guidance (**ICJG**) contains governing principles which are relevant to the guidance set out in this annex. However, not all of those principles are relevant here. The parts that are unlikely to be relevant are:

a) paragraph 1.4, which relates to illegal content judgements only and not fraudulent advertising judgements;
b) paragraphs 1.14- 1.19, which relate to illegal content safety duties as opposed to fraudulent advertising duties;
c) paragraph 1.23, which relates specifically to duties other than the fraudulent advertising duties;
d) box 1, paragraphs 1.24 – 1.27 and Figure 1.1. The box refers to 'illegal content' but is limited to 'regulated user-generated content' which cannot be a fraudulent advertisement. See the section titled 'Definition of fraudulent advertisements' below;
e) paragraphs 1.32-1.34, which relate to non-priority offences which are not relevant for the purpose of the fraudulent advertising duties;

[1] The Online Safety Act 2023 (Category 1, Category 2A and Category 2B Threshold Conditions) Regulations 2025.
[2] On a U2U service only, this is confined to paid-for advertisements that are not user-generated content.
[3] This requirement is set out in section 193 of the Act.

f) paragraph 1.38-1.39 which relate to facilitation of relevant offences. There is no equivalent fraudulent advertising duty relating to mitigating the risk of the service being used for the facilitation of a priority offence.

A3.5 All other parts of Chapter 1 of the ICJG are likely to be relevant and should be consulted. In those parts of Chapter 1 of the ICJG, references to 'illegal content' and 'illegal content judgements' should be read as references to 'fraudulent advertising' and 'fraudulent advertising judgements' respectively.

Category 1 and Category 2A services

A3.6 Duties regarding fraudulent advertisements (see paragraph A3.8) apply to Category 1 and Category 2A services only. Providers of other services are not required to make such fraudulent advertising judgements.

A3.7 Services fall into Categories 1 or 2A when they meet the conditions set out in The Online Safety Act 2023 (Category 1, Category 2A and Category 2B Threshold Conditions) Regulations 2025 (and summarised in Box 1). A full list of the services which meet such conditions is published in our Register of Categorised Services.[4]

Box 1: Overview of conditions and criteria for Category 1 and Category 2A services

CATEGORY 1 applies to services which meet either of the following criteria:

- The service uses a content recommender system *and* has more than 34 million UK users on the user-to-user part of its service; or
- The service allows user to forward or reshare user-generated content, *and* uses a content recommender system*, and* has more than 7 million UK users on the user-to-user part of its service.

CATEGORY 2A applies to services which meet both of the following criteria:

- The service is a search service, but not a 'vertical' search service;[5] and
- The service has more than 7 million UK users on the search engine part of its service.

Duties regarding fraudulent advertisements

A3.8 Service providers' duties regarding fraudulent advertising require them to:

[4] Ofcom, 2026. Register of Categorised Services.

[5] Vertical search services enable users to search for specific topics, or products or services offered by third-party operators with which they have a relevant arrangement (which may be contractual); these services could include flights, financial products or insurance. They differ from general search services in that they do not crawl the web for content or operate based on an underlying index, but instead return results through querying the individual operators' website or database directly. They do this by means of an API or equivalent technical means.

a) prevent individuals in the UK from encountering fraudulent advertisements by means of their service (Category 1 services) or in or via the search results of the service (Category 2A); [6]
b) minimise the length of time for which fraudulent advertisements can be encountered by individuals in the UK is present on their service (Category 1) or that it may be encountered by individuals in the UK in or via search results on the service (Category 2A); and
c) where they have been alerted to its presence, or become aware of it in any other way, swiftly take down fraudulent advertisements from their service (Category 1) or ensure that individuals in the UK are no longer able to encounter it via the service (Category 2A).

Definition of fraudulent advertisements

A3.9 In relation to a Category 1 service, content should be considered a fraudulent advertisement where it:

a) is a paid-for advertisement (see, paragraph A3.11);
b) is not regulated user-generated content[7] (see paragraph A3.12);[8] and
c) amounts to an offence as specified in section 40 of the Act – that is, 'fraud and financial services offences' as outlined in the Annex 2 accompanying this document, hereafter referred to as the '**fraudulent advertising offences**' (for more on 'amounts to an offence' see paragraph A3.13).

A3.10 In relation to a Category 2A service, content should be considered a fraudulent advertisement where it:

a) is a paid-for advertisement (see paragraph A3.11);
b) is encountered in or via the search results of the service; and
c) amounts to an offence as specified in section 40 of the Act – that is, 'fraud and financial services offences' as outlined in the Annex 2 accompanying this document (for more on 'amounts to an offence' see paragraph A3.13).

A3.11 Content is a paid-for advertisement if:

d) The service provider receives any monetary or non-monetary consideration for the advertisement being present on their service, whether directly from the advertiser[9] or from any other person; and

[6] It is important to note that encountering 'in or via search results' does *not* include instances in which fraudulent advertising is encountered because of subsequent interactions with an internet service *other than* the search service to which the duty applies.
[7] Some services display 'boosted' or 'promoted' content. Such content typically originates as and looks like user-generated content, but the user may have paid the service for the content to be boosted or promoted more widely beyond the user's followers. Multiple systems and processes can be involved in placing such content, including systems and processes related to user-generated content and paid-for advertising.
[8] Providers might consider (a) and (b) in either order.
[9] Advertisers may have multiple advertising accounts that can perform actions within an overall hierarchy, including a manager or parent account and individual accounts that perform specific actions. Advertising agencies can be contracted to carry out certain tasks, such as managing individual advertising campaigns and posting adverts.

e) The placement of the advertisement is determined by systems and processes that are agreed upon between the parties entering into a contract relating to the advertisement.[10]

A3.12 Content (including that which advertises goods or services) is user-generated content where[11]:

a) It is generated directly on the service by a user of that service, or uploaded to or shared on the service by a user of the service (including where it has been generated by means of software or an automated tool); and
b) It may be encountered by another user, or other users, of the service by means of the service.[12]

A3.13 Content will 'amount to an offence' where there are 'reasonable grounds to infer' that all elements necessary for the commission of the offence, including mental elements, are present or satisfied, and that there are no reasonable grounds to infer that a defence to the offence may be successfully relied upon. Guidance on how reasonable grounds to infer may be established is given in Section 2 of this annex.

Fraudulent advertising offences

A3.14 The fraudulent advertising offences are listed in section 40 of the Act. They broadly comprise:

a) False claims to be authorised or exempt for the purposes of carrying on regulated activity (the first of the financial services offences);
b) Fraud by false representation;
c) Fraud by abuse of position and participating in fraudulent business carried on by sole trader, etc.;
d) Other financial services offences;
e) Fraud related to misleading statements or impressions about investments;
f) Offences related to articles for use in fraud; and
g) Offences related to criminal property.

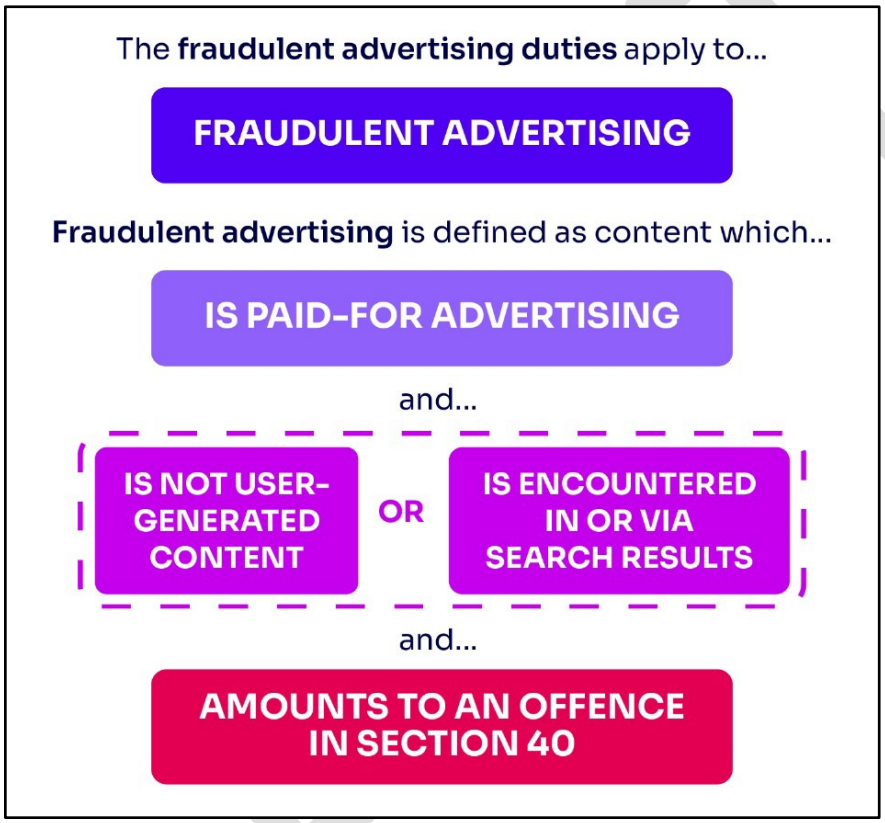
A3.15 It is also an offence to assist, encourage, attempt or conspire to commit one of the offences listed in section 40(2)-(4)[13] (or the equivalent offences in Scotland[14]), summarised above, or to aid, abet, counsel or procure the commission of one of these offences. In all these cases, an advertisement will only amount to a relevant offence (and therefore be a fraudulent advertisement) to the extent that the offence being encouraged, assisted,

[10] Section 236(1) of the Act.
[11] Section 55 of the Act defines "user-generated content".
[12] A 'bot' or other automated tool should be considered a user of the service, where: (a) the functions of the bot or tool in question include interaction with user-generated content; and (b) the bot or tool in question is not controlled by, or on behalf of, the service's provider. See section 55(4) of the Act.
[13] Encouraging could include words urging another person to carry out the offence. Assisting could include providing substantive help in carrying out the offence. There must either be intent to encourage or assist the offence, or belief that the offence will be committed. For conspiracy, there must be an agreement between two people and intent to carry out the offence.
[14] In Scotland, versions of these offences exist where a person incites another person to commit such an offence (section 40(6)) or is 'involved art and part' in the commission of such an offence (section 40(7)).

attempted or conspired to is sufficiently linked to the UK.[15] For more information on these forms of the fraudulent advertising offences, see paragraphs 1.29-1.31 and 6.18-6.19 of the ICJG.

A3.16 The relationship between fraudulent advertising and the offences listed in section 40 of the Act is set out in Figure A3.1.

Figure A3.1: How 'fraudulent advertising' relates to offences in section 40



[15] In determining whether an advertisement is 'sufficiently linked to the UK', the question is whether the UK would prosecute the people involved. The rules which decide whether or not there is a sufficient link are very complicated and content moderators cannot be expected to understand them in detail. However, for the purposes of this guidance, this requirement should be considered to be satisfied if the person being encouraged or assisted, or with whom there is a conspiracy, is either British or located in the UK.

A3.17 Service providers should also be aware that advertisements which do not meet the threshold to be considered paid-for fraudulent advertisements may still be considered misleading under the Digital Markets, Competition and Consumers Act 2024.[16] Advertisements which are misleading but not fraudulent are not within scope of the Act's duties. 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. The FCA deal with unclear or misleading advertisements in relation to financial products that are FCA regulated.[17] [18]

Reasonably available information

A3.18 Fraudulent advertising judgements should be made with reference to all information that is both relevant and reasonably available to a service provider.[19] This is not limited to the advertisement itself and also includes account level activity and any other available data. When making fraudulent advertising assessments, providers should apply the same principles as are set out in paragraphs 1.60-1.65 in Chapter 1 of the ICJG.

Information about the destination of an advert

A3.19 Many paid-for advertisements include a 'click-through' that opens a destination such as an external webpage ('**landing page**'), an in-service destination (such as a profile, storefront or product surface) or an on-app deep link (for example, to a product page in an e-commerce app or an app listing on Google Play or the App Store). On Category 2A services, these landing pages are considered part of the paid-for advertisement where encountered as a result of a single interaction with the advertisement in search results (such as by clicking on it). Webpages encountered through any subsequent interactions with an internet service other than the search service to which the duty applies are not considered part of the paid-for advertisement.

A3.20 On both Category 1 services and Category 2A services, we consider that information about the destination of an advert (including landing pages within a single interaction and, in more limited scenarios, other linked webpages) may constitute relevant and reasonably available information, depending on the circumstances. Relevant examples include:

- If a service provider is assessing whether the landing page matches the content of the advert (or is a cloned website impersonating something shown in the advert);

[16] Digital Markets, Competition and Consumers Act 2024 contains provisions to protect consumers from unfair trading. Source: Competition and Markets Authority Guidance. [accessed 3 June 2026].
[17] The ASA's Committees of Advertising Practice (CAP) non-broadcast code has rules that cover non-broadcast advertising (including online advertising). The rules are enforced by the ASA. To see the rules on misleading non-broadcast advertising see ASA CAP Code, Chapter 3: Misleading Advertising. [accessed 14 May 2026].
[18] The Financial Conduct Authority establishes binding rules on financial promotions through its Handbook; in particular, COBS 4.2 Financial Authority Handbook provides that firms must ensure communications are fair, clear and not misleading. This means that adverts should present information honestly and in a balanced way—for example, they should not exaggerate potential returns, downplay risks, omit important information, or use unclear language that could give consumers the wrong impression about a financial product.
[19] Section 192(2) of the Act.

- When a service provider is assessing whether the landing page has been altered after the advert was submitted or displayed; or
- If a link to a landing page or another linked webpage on that site has been included in a report to the provider about a suspected fraudulent advertisement.

A3.21 Where we consider information from landing pages to be relevant to fraudulent advertising judgements, we have indicated as such in a grey box outlining types of reasonably available information that should be considered. We are aware that many service providers employ automated URL-scanning technology, which allows click-through destinations to be scanned for potential threats, such as malware, phishing, or fraudulent activity such as the sale of counterfeit products or investment scams.

A3.22 Outputs from URL-scanning tools or services should be considered reasonably available information (and therefore factored into fraudulent advertising judgements) where they are relevant and reliable. In practice, this means that providers should undertake suitable due diligence and data assurance processes, and take reasonable steps to mitigate against the risk of incorrect detection outcomes. Service providers should also ensure that, where outputs suggest a URL destination is associated with fraud, the type of fraud concerned is relevant to the offences set out in section 40 (for example, an unregulated investment or consumer scam). Some types of illegal activity, such as the open advertising or sale of counterfeit goods, are not relevant to fraudulent advertising judgements but may be flagged by URL-scanning tools.[20]

Trusted flaggers

A3.23 Ofcom's draft Fraudulent Advertising Codes of Practice recommend that providers establish and maintain a separate reporting channel for the use of trusted flaggers. Service providers should take seriously any report from a trusted flagger within its area of expertise. They are entitled to assume that any evidence and information provided in such a report is true so far as the flagger concerned is aware, and that reasonable enquiries have been carried out. Except in the limited circumstances set out in paragraphs A3.39 to A3.40, which relate to financial services offences, a provider is not required to accept the opinions of such a third party as to whether advertisements are fraudulent advertising. Only a judgment of a UK court is binding on a provider in making this determination. In all other cases, it will need to take its own view on the evidence, information and any opinions provided.

Navigating the offences

A3.24 The offences outlined in paragraph A3.14 all relate to fraud and financial activity; however, there are material differences between the constituent parts of those offences, which will require different assessments to be made by providers. Service providers should therefore consider the most appropriate offence to start with based on the advertisement in question. The following example, which relates to financial services-related advertisements

[20] Providers should also consider their obligations under the Digital Markets, Competition and Consumers Act 2024, which require them to take steps to protect consumers from misleading commercial practices and ensure that their service does not enable consumer harm.

and offences, demonstrates how service providers can be directed to the starting point by considering the advert itself.

A3.25 If the advertisement includes a claim by a person (hereafter referred to as a '**firm**', which could include an individual) that it is authorised by the FCA or Prudential Regulation Authority ('**PRA**'), service providers should check the FCA's published list of authorised firms, available here as the Financial Services Register (the **FS Register**). A provider will have reasonable grounds to infer that a claim to be authorised is false and that it therefore amounts to one of the offences listed in section 40 of the Act if the firm is not included as an authorised firm on the FS Register or the details referred to in the advertisement do not match the details of the authorised firm on the FS Register.

A3.26 Once this check has been made, or if the advertisement does not contain a claim to be authorised, the most relevant offence to consider next will be fraud by false representation. Although this is an offence which requires providers to reasonably infer dishonesty, this is likely to be possible in some cases based on a consideration of the content of the advertisement in question.

A3.27 Other financial services offences may also be relevant. These are complex offences for which service providers will likely require a high degree of technical knowledge. In most cases, it will be appropriate for provider to rely on expert or external information when considering these offences or – where possible – to consider whether the advertisement in question also amounts to a fraud offence such as false representation.

Fraudulent advertising

A3.28 The process for carrying out a fraudulent advertising judgement varies for each offence. Where it is not clear which offence may be most relevant, we advise service providers to consider each of the fraudulent advertising offences sequentially, in the order they are presented below and in paragraph A3.14. Once they have reasonable grounds to infer that an advertisement amounts to any one offence, they need not consider any other offences.

A3.29 The factors to consider when making this judgement differ slightly from the equivalent factors which are relevant to making an illegal content judgement. As such, service providers should ensure that they are consulting the document which correctly corresponds to the type of judgement that they are making.

A3.30 When making fraudulent advertising judgements, service providers should consider whether they can reasonably infer that the advertisement in question amounts to any of the fraud or financial services offences set out in section 40 of the Act. [21]

A3.31 In the case of paid-for advertising content (see paragraph A3.11), where service providers can reasonably infer that the conduct and mental elements of the offence are satisfied, and there are no reasonable grounds to infer that a relevant defence may be successfully relied upon, they should find that the content amounts to any of the fraud or financial services offences set out in section 40 of the Act. [22]

[22] Section 192(6) of the Act.

A3.32 For more information on how service providers should approach the 'reasonable grounds to infer' threshold, including the role played by reasonably available information, see paragraphs 1.40-1.47, 1.51-1.55 and 1.57-1.59 of the ICJG.

Fraudulent advertising offences

False claims to be authorised or exempt for the purposes of carrying on regulated activity

A3.33 We have separated this offence from the rest of the financial services offences and presented it first, before fraud by false representation, because, compared to the other financial services offences, it is relatively easy to make reasonable inferences regarding false claims to be authorised or exempt. The guidance in the rest of this section is broadly divided into three parts: 1) fraud by false representation, 2) financial services offences and 3) other fraud offences.

A3.34 This section relates to advertisements which appear to involve the provision or promotion of financial products or services (e.g., investments, insurance, mortgages, credit) and relevant claims management businesses. It deals with false claims to be authorised or exempt for the purposes of carrying on regulated activity, which is one of the priority offences from the Financial Services and Markets Act 2000 (**FSMA**).

When the content claims to be made by an FCA - or Prudential Regulation Authority-authorised person

A3.35 Where content claims to be made by a person authorised by the FCA or Prudential Regulation Authority (**PRA**) , service providers should follow the steps outlined:

a) Providers should first determine whether it can be reasonably inferred that the advertisement contains a claim by a firm to be authorised by the FCA or PRA.
b) If this can be inferred, providers should next identify the name of the firm claiming to be authorised.
c) When identified, the name of the relevant firm should be checked against the FS Register. Service providers should check the status of a firm as listed on the FS Register to determine whether they are authorised.

A3.36 The FS Register is updated regularly and provides information on whether firms are authorised by the FCA and the PRA.

A3.37 It is important to remember that the FS Register includes information about a number of different categories of person and not just authorised persons. For example, the FS Register also includes details of appointed representatives, registered crypto asset firms and electronic money and payment services firms. Such persons will not necessarily be authorised persons. To check whether a person is authorised, service providers should therefore be careful to ensure that the FS Register shows the status of 'authorised'.

A3.38 When service providers review the FS Register, they should check the details carefully to ensure the name and details match the name and details associated with the content. Providers should be alert to the activities of 'clone firms'.[23]

A3.39 A service provider will have reasonable grounds to infer that a claim to be authorised is false and that an advertisement amounts to one or more of the offences in section 40 if the firm is claiming to be authorised by the FCA or PRA, but is not included as an authorised firm on the FS Register or if the details referred to in the online content do not match the details of the authorised firm on the FS Register. Providers should ensure that they have identified a false claim to be authorised. A person operating as an appointed representative or payment services firm, for example, may be lawfully engaged in financial services activity, but in this case they will not claim to be authorised themselves. False claims to be authorised are likely to be made using language such as 'authorised and regulated by… [the FCA, the PRA, etc.]'.

A3.40 Particular care should be taken when a firm is listed on the FS Register as unauthorised (usually in red) or included in the FCA Warning List here. Firms in red in the FS Register, or included on the Warning List, are unauthorised persons which the FCA is concerned are carrying on regulated business unlawfully. The FCA Warning List is a list of unauthorised firms and individuals that the FCA has identified may be providing services or products in a way which would amount to one or more FSMA priority offences. For more information on the use of the FCA's Warning List, see paragraphs A3.84-A3.85.

A3.41 Providers of in-scope services should note that the unauthorised firms listed on the FS Register or included in the FCA Warning List are not exhaustive. The FCA will add firms to the FS Register and Warning List as soon as possible. However, if a firm is not on the list, it could still be committing an offence.

When the content claims to be by an appointed representative

A3.42 In circumstances where the advertisement refers to a firm or individual acting as appointed representative of another firm or individual, providers should check the FS Register to establish whether the appointed representative is listed as a relevant current appointed representative. If they are not included on the FS Register, or if the information about the appointed representative's principal does not match that on the Register, it is reasonable for service providers to infer any person doing so is not, in fact, an appointed representative. In these cases, there will be reasonable grounds to infer that the advertisement amounts to an offence in section 40.

Usage examples

- A company which does not appear on the FS Register, or whose entry does not say it is 'authorised', publishes content in which it says it is 'authorised and regulated by the FCA'.

[23] Clone firms are impersonations or copies of FCA- or PRA-authorised firms. Bad actors use clone firms to provider a cover of legitimacy, tricking potential investors into believing that they are being offered an investment by a trustworthy source. Often, bad actors will use the names, addresses and financial registration number (FRN) of an authorised firm as part of their attempt to deceive potential investors.

Reasonably available information for Category 1 and Category 2A services

- The advertisement suspected to be a fraudulent advertisement.
- Information provided by any complainant in a free text box, including information from any person the provider considers to be a trusted flagger.*
- Information from the FS Register or FCA Warning List.

*A provider should accept the opinions of the FCA and PRA as to whether a person is authorised by them. However, the opinions of a third party are not determinative as to whether the post amounts to a claim to be authorised. Only a judgment of a UK court is binding on the provider in making this determination. A provider will need to take its own view on the evidence, information and any opinions provided.

References

Legal annex: Section A7 of Annex 1.

Statute: Section 24 of the Financial Services and Markets Act 2000.

Fraud by false representation

A3.43 This section includes the priority offences of fraud by false representation, fraud by abuse of position and the sole trader offence.[24] Fraud by abuse of position is likely to be less identifiable in paid-for advertisements on Category 1 and 2A services. Furthermore, it is difficult to imagine circumstances where an advertisement amounting to both this offence and participating in a fraudulent business carried on by a sole trader would not also amount to fraud by false representation (for these offences, see A3.78). Service providers should therefore consider fraud by false representation first of all, and we have provided the most substantive guidance on this offence.

A3.44 It is an offence to 'dishonestly make a false representation' where the person making such a representation intends to make a gain thereby (for themselves or others) or to cause another person loss (or expose them to the risk of loss). An advertisement should be considered to amount to an offence in section 40 where there are reasonable grounds to infer that it contains a false representation (see paragraph A3.52-A3.57) that was made dishonestly for *either* of these two purposes. For reasonable grounds to infer to be reached, providers do *not* need to infer that the representation resulted in an actual gain or loss, only that this was possible.

A3.45 It will not be possible for providers to identify all instances of advertising amounting to this offence. A service provider will not always be in a position to know whether a representation is false, what the intent of the person is in making it, or whether they were dishonest. However, in some cases, it will be appropriate for providers to draw these inferences. In practice, service providers will likely need to consider the same factors when making reasonable inferences about both the conduct and the state of mind elements of an offence. That is, providers are likely to need to consider the same factors when considering:

[24] Sections 2, 4 and 9 of the Fraud Act 2006.

a) whether a representation is false and
b) whether the advertiser knew the representation to be false and had dishonest intent.

A3.46 For example, factors which suggest dishonesty – such as use of apparently deliberately misspelled words or unprintable characters – may also suggest that a representation is false. Effort made to evade moderation suggests that the advertiser knows that the representation being made is false. Similarly, any representation claiming unrealistic levels of return can be reasonably inferred to be false, and this may suggest dishonesty. This is because it is reasonable to assume that anyone offering an investment product would know the rates of return to be unreasonable.

A3.47 In this section, we set out the main concepts of the offence: false representations, dishonesty and intention to make a gain a loss. We then describe how service providers might approach them in practice. For an advertisement to amount to the fraud by false representation offence, four things are needed:

a) There must be some sort of a representation, likely information within the advertisement itself;
b) There must be some information which suggests the representation made is false;
c) There must be some information which could lead to a loss or gain; and
d) There must be some information which suggests that the person posting the content is doing so dishonestly.

A3.48 It is important to note that identifying fraud online is particularly challenging and there is unlikely to be one factor alone that that indicates that an advertisement amounts to an offence of fraud by false representation. Instead, a combination of factors will indicate this.

User reporting and fraud by false representation

A3.49 User reports, especially those from trusted flaggers, are likely to be particularly important in alerting service providers to untrue or misleading representations. Where reports by trusted flaggers and / or user reports are available to a provider regarding the contents of an advertisement, it should consider these as appropriate.

Reviewing reasonably available information for fraud by false representation

A3.50 In the first instance, a service provider should assess the primary information. This includes the advertisement in question, and any complaint that may have been made about it (including supporting evidence from the complainant). If a provider is unable to make an assessment based on this primary information, then they should consider supplementary information as listed in the appropriate reasonably available information box.

A3.51 The reasonably available information that a service provider takes into consideration should be appropriate for the fraud type in question.

What is 'a false representation'?

A3.52 A false representation is a representation (for example, a statement, suggestion, comment, inducement, etc.) which is untrue or misleading and the person making it knows that it is or might be untrue or misleading. It can be expressed or made clear without explicit language, e.g., through the use of imagery or symbols.

A3.53 A representation can be made in any medium. It could appear in content as written material, photographs, videos, visual images, oral communication, data, titles and descriptions.

A3.54 Online advertisements are capable of making a 'representation' as, by their very nature, they use words, imagery and symbolism to convey information to a potential customer. However, the 'representation' must consist of some kind of claim in the advertisement itself: for example, by stating the features or benefits of a product or service, advertising a product or service as available to purchase for a set price, or suggesting that the product or service is endorsed by a public figure.

A3.55 The representation does not need to be made to another person. There may be reasonable grounds to infer that an advertisement amounts to an offence of fraud by false representation even where a person makes a representation to a machine or a piece of software which is able to respond without any need for human involvement. The representation will be made only when the content is transmitted.

A3.56 We recognise that making inferences about what is true in an online context may be challenging for service providers. In many cases, providers will not be able to ascertain the facts of the case. However, it may be possible for providers to infer that a representation is false, from information they have available.

A3.57 Where service providers are considering an advertisement which uses a URL link to make a potentially false representation, they can mitigate potential security risks of accessing any landing page by using an automated URL-scanning technology or URL-checking service.

Dishonesty

A3.58 For content to amount to this offence, there must be reasonable grounds to infer that the false representation was made dishonestly. The question of whether the conduct can be reasonably inferred to be dishonest is determined by applying the standards of 'ordinary decent people'.[25] If dishonesty cannot reasonably be inferred, the advertisement should not be judged to amount to an offence of fraud by false representation.

A3.59 We recognise that making inferences about dishonesty in an online context is particularly challenging because in many cases, service providers will not be able to ascertain the actual state of knowledge or belief as to the facts relating to the individual or individuals who have posted the advertisement. However, it is possible for providers to *infer* such an individual's knowledge or belief as to the facts from the nature of their content or behaviour online.[26]

A3.60 In certain circumstances, it may be easier to do this than in others. For example, it might be possible to reasonably infer dishonesty on the face of the content itself in some cases such as:

- An advertisement which uses manipulated or AI-generated content of a public figure, where the person depicted is known not to advertise or endorse individual products;[27] or

[25] This phrase is taken from case law regarding the meaning of dishonesty in a legal setting.

[26] By online behaviour, we mean actions taken by users (other than posting content) which may be against a service's terms. Examples include using bots, fake accounts or 'bot farming' to artificially inflate follower numbers; adding a user to a group or group chat without their consent; or unsolicited 'tagging'.

[27] One example is Martin Lewis, who has made a public declaration on this. Source: Money Saving Expert (Sproson, K.), 2026. Martin Lewis scam adverts. [accessed 14 May 2026].

- An advertisement which contains a claim about something that an advertiser could not reasonably know, such as a user's computer being infected with a virus.

A3.61 In cases such as these, the service provider can reasonably infer that the advertisement has been created dishonestly and it should take action.

A3.62 In cases where the dishonesty is not quite as clear on the face of the advertisement, other reasonably available information may be relevant.

A3.63 Where agents are involved in the submission of advertisements, service providers can infer dishonesty to either the agent or the advertiser as appropriate.[28]

A3.64 Providers should not be deterred from taking action on an advertisement because they are unsure who holds the dishonest intent, for example, as a result of the involvement of an agent in submitting the advertisement.

Intention to make a gain or to cause another person loss

A3.65 It is also a requirement of this offence that the person making the false representation did so intending to make a gain or to cause a loss to another or to expose another to a risk of loss. It does not matter if no actual gain was made or loss caused. The requirement is only that the person intended either of these things to happen.

A3.66 Service providers should consider this criterion met where the advertisement contains a representation which requests or induces a payment or investment to be made, or otherwise encourages a transfer of value. In these instances, it will be reasonable to infer an intention to make a gain or cause a loss by virtue of the advertisement having been submitted to the service's advertising platform.

A3.67 The ultimate purpose of most advertising is to encourage consumers to purchase goods or services which will result in profit for a business or organisation, or to otherwise part with money or another form of value in some way to this same end. As such, most advertisements will contain an intention to make a gain or cause another person a loss. However, there will be some instances where this is not the case, such as genuine non-fundraising awareness-raising campaigns by arms-length bodies (such as public health bodies or executive agencies such as the DVLA) and government departments.

Identifying content which amounts to fraud by false representation

A3.68 It is unlikely that one factor alone will give rise to reasonable grounds to infer that content amounts to a fraud by false representation. Instead, service providers will need to consider a range of factors. Often a factor that is relevant to one part of the offence is also relevant to another. For example, the information which allows a provider to infer that there has been a false representation or an intent to make a gain may also be the grounds for inferring dishonesty.

A3.69 Offenders' tactics are particularly likely to change over time and be prompted by real-world events, and so service providers will need to be alert to the many different ways in

[28] Advertisers may have multiple advertising accounts that can perform actions within an overall hierarchy, including a manager or parent account and individual accounts that perform specific actions. Advertising agencies can be contracted to carry out certain tasks, such as managing individual advertising campaigns and posting adverts.

which false information may be dishonestly used to make a gain or cause another a loss. It is ultimately up to providers to stay up to date with new indicators.

A3.70 In the guidance below we have provided illustrative examples of red flag indicators of fraud by false representation (**red flag indicators**) to assist service providers to identify advertisements amounting to an offence of fraud by false representation. These indicators are not exhaustive. The main point to note is that to identify fraud by false representation, service providers should not look for just one factor but instead look at a combination of factors. It is important to underline that the majority of the examples provided are not, in isolation, capable of providing reasonable grounds to infer that advertising content amounts to an offence.

Contextual factors common in advertisements amounting to fraud by false representation

A3.71 Besides the illustrative examples we set out further below under each heading, service providers may identify other contextual factors that are sometimes present in advertisements amounting to fraud by false representation. On their own, these factors should not be treated as evidence that an advertisement amounts to that offence. However, presence of any of these factors may be useful in helping to identify an advertisement as a priority for review, or as needing further checks (for example, review through human moderation, or use of a URL-checking tool to see if a URL landing page associated with the advertisement has been identified as fraudulent). These contextual factors, therefore, indicate the need to subject the advertisement to a more in-depth fraudulent advertising judgement against the fraud by false representation offence, rather than providing reasonable grounds to infer fraud by false representation in themselves. As with red flag indicators, a provider would need to stay up to date with new contextual factors.

A3.72 Examples of this sort of contextual factor are:

a) Use of wealth signifiers (e.g., currency, luxury cars, private airplanes, snapshots of bank accounts), where these are being used to back up claims about investments.
b) Sensationalist headlines about celebrities.
c) Edited, decontextualised or inauthentic images; AI-generated images or celebrity images; or images used in conjunction with a link prompting users to move off site.[29]

A3.73 Service providers should take a pragmatic approach which considers whether it is more reasonable overall to infer that a dishonest false representation has been made than it is to assume the opposite.

Red flag indicators

Information which suggests the representation is false

A3.74 The examples of specific information have been mapped against four overarching categories to ensure clarity. The following are examples of representations which may be made through fraudulent advertisements:

- A claim that an investment or the firm concerned is regulated.

[29] This may include images which are not inauthentic or AI-generated, but which have been removed from their original context and re-presented in a way which is intended to support a false claim.

- A claim that an investment or the firm concerned is regulated by a body which does not exist (this is a particularly serious example and is very likely to be associated with a fraud).
- A claim that a product is endorsed by a public figure or well-known organisation, unless it is obviously done as a parody.
- A claim that an investment provides a 'specific' return.
- A claim that a product (for example, a drug, medical product or weapon) is approved or legal to be sold in all circumstances in the UK (for example, without a licence or prescription), including by use of accreditation symbols or logos associated with provision or licencing of that type of product.
- A claim that the advertiser is authorised to advertise a product (where the ability to do so is restricted).

A3.75 Service providers should be aware of the following indicators below, which may suggest that the representation is false.

Content-specific anomalies:

a) Content guaranteeing an obviously unrealistic rate of return within the time frame for investment or current environment, or which otherwise seem 'too good to be true'.
b) Highly unrealistic discounts or prices.
c) Posts using enticing language to suggest unrealistic gains; for example, 'easy money' or 'fast cash'.
d) Use of 'deepfake' technology, particularly to represent a public figure who is endorsing the product or service being advertised.
e) Language which exerts pressure on those being requested to send money or invest, including time pressure which is not warranted. Note: this could also suggest dishonesty.
f) A claim that an opportunity has arisen, and that quick action is required to benefit from it.

Links to accounts that have been found to have posted fraudulent advertising to UK users:

a) The advertising account submitting the advertisement shares identifiable characteristics with an advertising account that has already been identified as having posted a fraudulent advertisement. For example, the accounts may share the same phone number, IP address or device identifier, password, registered business address or residence, or named contact. However, service providers should always consider whether there is a legitimate explanation or reason for these similarities.

Historical and current reports and complaints:

a) Accounts that are frequently flagged or reported by users, particularly through dedicated reporting channels used by trusted flaggers, unless the flags appear to be malicious (e.g., made by competitors).
b) An advertisement which has been flagged as fraudulent by an account (either personal or affiliated with a well-known organisation) that is part of a notable user account verification scheme should be treated as particularly likely to be problematic.
c) Results from automated scanning technology tools or services which suggests that a URL included in the advertisement (including as an embedded click-through link) has been associated with fraudulent activity.

Information which could lead to a loss or gain

A3.76 Most advertisements will contain an intention to make a gain or cause another person a loss. However, paragraphs A3.67 give possible exceptions to this.

Information which suggests that the person submitting the advertisement is doing so dishonestly

A3.77 Service providers should be aware of a number of characteristics commonly associated with fraudulent behaviour:

a) All points set out under 'Information which suggests the representation is false'.
b) The use of apparently deliberately misspelt words or non-printable characters to evade automated filters (e.g., '0ne million d0llars' or characters which are read by computers but not displayed to users).
c) Claims that the investment or firm concerned is regulated by a body which does not exist. (This is a particularly serious example and is very likely to be associated with a fraud.)
d) Use of a username or account name which is similar to, or able to be mistaken for, that of a username or account owned or operated by a brand, company or public figure.
e) Use of brand identity or the likeness of a person, where characteristics of the account submitting the advertisement are inconsistent with known characteristics of the brand or person concerned (for example, an account with an IP address outside the UK using the branding of a UK-based business in its advertisement in a way which suggests the product or service being promoted is associated with that business).

Note on usage examples

We have not given any usage examples here, due to the particularly strong importance of context to these judgements. Service providers should refer to the lists of factors in paragraph A3.72 when identifying examples of content which are likely to meet the threshold of reasonable grounds to infer that an advertisement amounts to the offence.

Reasonably available information for user-to-user services

Primary information

- The advertisement suspected to be a fraudulent advertisement.
- Any complaint and supporting information provided by any complainant, including that which is provided by any person the provider considers to be a trusted flagger, or by a verified account which the account posting the suspected fraudulent post is copying.*
- Where available, results from automated scanning technology tools or services which suggests that a URL included in the advertisement (including as an embedded click-through link) has been associated with fraudulent activity.

Supplementary Information

- Metadata such as location, time of posting and IP address.

- Information on previous advertiser activity, including whether previous submissions have been judged to be fraudulent.
- Account profile information, such as the username, user image and any contact details or reference number.
- Information on previous complaints about advertisements posted by the same advertising account.
- A reverse image search, where a complaint is received which suggests an image is inauthentic or taken out of context.

*A provider is not required to accept the opinions of a third party as to whether an advertisement is fraudulent advertising. Only a judgment of a UK court is binding on it in making this determination, in that it will provide clear evidence that the advertisement in question amounts to a relevant fraud offence. In all other cases, it will need to take its own view on the evidence, information and any opinions provided.

Reasonably available information for search services

Primary Information

- The content suspected to be a fraudulent advertisement encountered in search results and/or the content suspected to amount to an offence in section 40 that is encountered because of interacting with a paid-for advertisement in search results.
- Any complaint and supporting information provided by any complainant, including that which is provided by any person the provider considers to be a trusted flagger, or by a verified account which the account posting the suspected fraudulent post is copying.*

Supplementary Information

- Metadata such as location, IP address and domain name details.
- Information on previous complaints about the same search content or website.
- A reverse image search, where a complaint is received which suggests an image is inauthentic.

*A provider is not required to accept the opinions of a third party as to whether an advertisement is fraudulent advertising. Only a judgment of a UK court is binding on it in making this determination. In all other cases, it will need to take its own view on the evidence, information and any opinions provided.

References

Legal annex: Section A7 of Annex 1.

Statute: Section 2 of the Fraud Act 2006.

Case law: *Ivey v Genting Casinos (UK)* (trading as Cockfords Club) [2017] UKSC 67.

Other: Information about enforcement action against online service providers under consumer protection legislation is available at Competition and Markets Authority cases and projects.

Fraud by abuse of position and participating in fraudulent business carried on by sole trader, etc.

A3.78 Two further fraud offences are less likely to be identifiable on in-scope services. Paid-for advertising content amounting to these offences would in any event be likely to amount to an offence of fraud by false representation. For completeness, these are set out in Chapter 6 of the ICJG (see pp.112-113).

Other financial services offences (excluding false claims to be authorised or exempt)

A3.79 We have already dealt with content amounting to false claims to be authorised or exempt for the purposes of carrying on a regulated activity, which is one of the fraudulent advertising offences from the Financial Services and Markets Act 2000. Where reasonable grounds do not exist that content amounts to an offence mentioned in the previous sections, but the content in question appears to involve the provision or promotion of financial products or services (e.g., investments, insurance, mortgages, or credit) or claim management activity, service providers should next consider whether the content amounts to one of the other FSMA offences. These include:

- Contravention of prohibition on carrying on regulated activity in the UK unless authorised or exempt; and
- Contravention of restrictions on financial promotions.

A3.80 We refer to these offences, together with the offence of false claims to be authorised or exempt for the purposes of carrying on regulated activity, as the **FSMA fraudulent advertising offences**.

Persons neither claiming to be authorised nor an appointed representative

A3.81 In many cases, online content encountered by providers that may amount to FSMA fraudulent advertising offence will not contain any claim by a firm or individual to be either authorised or an appointed representative. Of the two remaining FSMA offences, service providers are most likely to encounter advertisements amounting to an offence of contravening restrictions on financial promotions, as online advertisements are not commonly used to carry out regulated financial services activity.

A3.82 These offences involve a high level of technical complexity, which will require specialist expertise. Service providers with their own legal teams may find more information on FSMA offences by consulting the FCA Handbook,[30] and Annex 3 accompanying this annex.[31]

A3.83 In addition to cases where an identified firm or individual appears on the FCA Warning List (see paragraphs A3.84-A3.85), service providers have reasonable grounds to infer that an advertisement amounts to a FSMA priority offence where:

a) The FCA or PRA provides them with an explanation of why, in its opinion, each part of the FSMA priority offence concerned is present or satisfied; unless

[30] See particularly: Financial Conduct Authority, 2005. FCA Handbook: PERG 8.23 Regulated activities. [accessed 24 March 2026].
[31] See A2.6 in Annex 2.

b) An individual at the service provider who is reviewing the opinion is aware of evidence to the contrary, which is unavailable to the FCA or PRA.[32]

Use of the FCA's warning list

A3.84 Service providers should also pay particular attention to the inclusion of firms and individuals on the FCA Warning List. The FCA Warning List is a list of unauthorised firms and individuals that the FCA has identified may be promoting or providing financial services or products in breach of one or more FSMA fraudulent advertising offences. A firm's or individual's presence on the Warning List may be taken as reasonable grounds to infer that the expert regulator has looked at the person's activities and concluded that they appear to be committing one or more offences. However, the fact that a person is not included on the list should not be considered proof that a person is operating lawfully.

A3.85 Where an advertisement is for financial services and it is possible to identify a particular firm or individual who appears to be promoting it , service providers should check the name of the firm or individual in question against the Warning List. Where the name is identified as a person who may be providing financial services or products without authorisation, providers will have reasonable grounds to infer that content amounts to a FSMA offence, except where the provider has evidence to suggest the contrary.

Note on usage examples

We have not given any usage examples here, due to the particular complexity of the offence. Service providers should have regard to information provided to them by bodies mentioned in paragraph A3.83.

Reasonably available information for user-to-user and search services

- The advertisement suspected to be fraudulent.
- Information on the FCA's Warning List.
- Supporting information provided by any complainant, including that which is provided by any person the provider considers to be a trusted flagger.*

*A provider should consider the opinions of the FCA or PRA as to whether an advertisement amounts to a FSMA fraudulent advertising offence included in section 40 of the Act. Otherwise, only a judgment of a UK court is binding on it in making this determination. In all other cases, it will need to take its own view on the evidence, information and any opinions provided.

References

Legal annex: Section A7 of Annex 1.

Statute: Sections 19, 21, 23 and 25 of the Financial Services and Markets Act 2000.

[32] This guidance focuses on the circumstances in which all service providers will have reasonable grounds to infer that content amounts to an offence. Providers that engage with specialists and with the full technical complexity of the offences might identify a wider range of circumstances.

Misleading statements and impressions about investments

A3.86 Also included in the list of fraud offences at section 40 of the Act is the offence of making a false or misleading statement (or concealing facts), or creating a false or misleading impression, in connection with a relevant agreement or relevant investment.

A3.87 In practice we are currently unaware of any examples on in-scope services of the offence of creating a misleading impression about an investment with the intention of inducing another person to do or not do something in relation to that investment. This section therefore focuses on misleading statements.

A3.88 For an advertisement to be considered fraudulent by virtue of this offence, there must be reasonable grounds to infer that the following criteria are met:

a) Either:

i) a person makes a statement in relation to which either of the following is true:

a. they know it to be false or misleading in a material respect; or
b. they are reckless as to whether the statement is false or misleading in a material respect; or

ii) whether in connection with a statement made by them or otherwise, the person dishonestly conceals any material facts.

b) The person does any of the acts in point a) with the intention of inducing or is reckless as to whether doing any of the above actions may induce another person to:

i) enter into, offer to enter into, or to refrain from entering or offering to enter into, a relevant agreement, or

ii) exercise, or refrain from exercising, any rights conferred by a relevant investment.

A3.89 A possible example of this offence occurring in paid-for online advertising is an advertisement for an investment which makes a claim of guaranteed returns of a certain percentage, without there being any reasonable basis for this claim, or claims that an advertisement is 'risk-free'.

A3.90 The offence poses a particular challenge to fraudulent advertising judgements because of its high level of technical complexity. Service providers with their own legal teams may find more information in the Annex 2 accompanying this guidance.[33]

A3.91 However, in most cases, a service provider is likely to become aware that a statement meets the criteria set out in paragraph in A3.88 only when it has been alerted to this by specialist third parties (such as law enforcement after a successful prosecution) or by a regulator with appropriate expertise (such as the FCA).

Note on usage examples

We have not given any usage examples here, due to the particularly strong importance of context to these judgements.

[33] See particularly: Financial Conduct Authority, 2005. FCA Handbook: PERG 8.23 Regulated activities. [accessed 19 September 2023].

Reasonably available information for user-to-user and search services

- The content suspected to be fraudulent advertising.
- Supporting information provided by any complainant, including that which is provided by any person the provider considers to be a trusted flagger.*
- Where available, results from automated scanning technology tools or services which suggests that a URL included in the advertisement (including as an embedded click-through link) has been associated with fraudulent activity.

* A provider should consider the opinions of the FCA or PRA as to whether content amounts to a FSMA priority offence in accordance with paragraph 6.74. Otherwise, only a judgment of a UK court is binding on it in making this determination. In all other cases, it will need to take its own view on the evidence, information and any opinions provided.

References

Legal annex: Section A7 of Annex 1.

Statute: Sections 89 and 90 of the Financial Services Act 2012.

Articles for use in frauds

A3.92 This section looks at the priority offence of making or supplying articles for use in frauds. We note that we have only provided usage examples in the section dealing with articles for use in fraud. Most other offences are so context-specific that usage examples are not likely to be helpful.

A3.93 It is an offence to make, adapt, supply or offer to supply any article, knowing that it is designed or adapted for use in the course of or in connection with fraud. It is also an offence to make, adapt, supply or offer to supply any article, intending that it be used to commit, or assist in the commission of, fraud.

A3.94 Articles need not be tangible things. They can include data, for example, lists of other people's stolen credit or debit card information, personal identification numbers (PINs) or passwords, and software or programs.[34] Data of this kind is commonly advertised for sale using the term 'fullz'[35] or 'dump':[36] for example, in phrases such as 'PIN dump' or 'credit card dump'.

A3.95 In practice, most 'making', 'adapting' and 'supply' of tangible items (that is, items other than data) will take place offline. Online advertising content is most likely to amount on

[34] Such software or programs may include card-skimming software or apps.
[35] The term 'fullz' is commonly used by bad actors to identify data that are sold or traded. It is short for 'full information'. A 'fullz' file typically comprises of complete set of information about an individual or individuals which might include their name, address, date of birth, credit card number, expiration date, card security code and other personal information. This can then be used for identity theft and other types of fraudulent activity.
[36] The term 'dump' is commonly used by bad actors to refer to information contained on the magnetic stripe of a credit or debit card. This will typically include the owner's name, card number and expiration date. Dumps are usually stolen using malware on point-of-sale (PoS) systems. Every card which is used on those terminals is copied and transferred to a bad actor who may then use this information themselves or sell it on as a 'dump' for purchase by others.

'offer to supply'. For the purposes of this offence, 'offer' should be given its ordinary English meaning, rather than any more precise meaning that exists in contract law.

A3.96 For an advertisement to amount to the articles for use in fraud offence, it must be reasonable to infer that the individual submitting or creating the advertisement intended that the article in question be used to commit or assist in the commission of fraud. It is not uncommon for people posting to be open about the likely use of articles offered for supply online, and in some cases this may include open promotion through paid-for advertising. Service providers should infer knowledge and intent where the advertisement states that the article may be used for fraud, unless what is said is obviously a joke.

A3.97 Otherwise, when considering state of mind, service providers should ask themselves whether there is any possible use of the article concerned which is not for fraud, and how likely it is that use of it would not be for fraud. If it is more likely than not that the article is for use in fraud, then there will be reasonable grounds to infer that the advertisement amounts to this offence. If any non-fraudulent use would still be illegal, then service providers should also take the view that the reasonable grounds to infer exist.

Usage examples

- An advertisement for a fake passport or other identity document (most fake passports are provided for use in social security fraud).
- An advertisement offering to sell (or otherwise supply) passwords.
- An advertisement offering to sell (or otherwise supply) Bank Identification Numbers (BINs) – the first six digits of a credit or debit card number, which determines card issuer, card type, level of security and country of origin.
- An advertisement offering to sell (or otherwise supply) data loaded onto a credit card's magnetic strip, including bank account number, cardholder name, expiration date, service code and personal identification number (PIN) – often referred to as 'dump'.
- An advertisement offering to sell (or otherwise supply) a full set of personal information, including date of birth, mother's maiden name, email, home address, phone number, etc., often described as 'fullz'.
- An advertisement for a 'fraud bible' or any sort of instruction manuals providing guidance on how to carry out fraudulent activity.
- An advertisement offering to sell an online advertising account, outside of formal business restructuring or provider-approved processes.

Reasonably available information for user-to-user and search services

- The advertisement suspected to be fraudulent advertising.
- Supporting information provided by any complainant, including that which is provided by any person the provider considers to be a trusted flagger.*

*A provider is not required to accept the opinions of a third party as to whether an advertisement is fraudulent advertising. Only a judgment of a UK court is binding on it in making this determination. In all other cases, it will need to take its own view on the evidence, information and any opinions provided.

References

Legal annex: Section A7 of Annex 1.

Statute: Section 7 of the Fraud Act 2006; section 49(3) of the Criminal Justice and Licensing (Scotland) Act 2010 (articles for use in fraud).

Caselaw: *R v Dhillon* [2000] Crim LR 760.

Offences related to criminal property

A3.98 There are also priority offences relating to criminal property, including offences relating to the sale of stolen goods or the sale of items which facilitate theft. In practice, we are aware of few circumstances in which paid-for advertisements would amount to these offences.

A3.99 However, service providers should consider whether content amounts to an offence of assisting a person to do any of the acts outlined in A3.93. For example, advertisements may assist in the sale of items which facilitate theft where they advertise products such as key jammers, RFID copiers, or ATM skimmers for sale.[37] In rare cases, advertisements may also enable the sale of stolen goods where they offer goods of some kind for sale and it is clear on the face of the advertisement that these goods have been stolen. An example would be the sale of stolen credentials.

Usage example

- An advertisement offering stolen credentials for sale, where it is clear that they are stolen.
- An advertisement offering an item such as a key jammer, ATM skimmer or for sale.

Reasonably available information for user-to-user and search services

- The advertisement suspected to be fraudulent advertising.
- Supporting information provided by any complainant, including that which is provided by any person the provider considers to be a trusted flagger.*

* A provider is not required to accept the opinions of a third party as to whether an advertisement is fraudulent advertising. Only a judgment of a UK court is binding on it in making this determination. In all other cases, it will need to take its own view on the evidence, information and any opinions provided.

[37] A key jammer is an electronic device used by thieves to gain entry into vehicles without setting off the alarm system. They work by disrupting or blocking the signal from a vehicle owner's key fob, preventing the car from locking when the owner has attempted to do so by using the fob. An RFID copier is a device which scans and stores the signal from vehicle key fobs, allowing thieves to reproduce the signal and enter the vehicle without force. An ATM skimmer is an electronic device which can be affixed to an automated teller machine (ATM, or cashpoint) to obtain debit card details, including PINs.

References

Legal annex: Section A7 of Annex 1.

Statute: Section 327, 328 and 329 of the Proceeds of Crime Act 2002.