Fraudulent Advertising Codes Consultation

Volume 1: Context

Consultation

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

For more information on this publication, please visit ofcom.org.uk

Contents

Section

1. Overview

What are we doing today?

1.1 The Online Safety Act 2023 (the Act) requires certain online services to have in place greater levels of transparency and accountability, empower users with more choice and control, and protect users from fraudulent advertising.

1.2 These services, known as categorised services, are some of the most widely used online services in the UK. Ofcom, as the online safety regulator, is responsible for ensuring that providers of these services comply with the additional responsibilities placed upon them.

1.3 We are publishing our proposals for what Category 1 and Category 2A services should do to tackle fraudulent advertising in line with their duties under the Act. The proposals apply to paid-for advertising content, and not user-generated content (UGC) or non-sponsored search content.

1.4 We are also publishing our register of categorised services, and our proposals for additional duties on Category 1 services.

What is the FAC Consultation?

1.5 The UK's digital advertising market surpassed £40.5bn in 2025.[1] It is a highly profitable segment, especially for the largest players.[2]

1.6 Fraud is the most common crime in the UK, and the economic and social costs are substantial (c.9.2bn).[3] Fraudulent advertising online is a major part of the problem. Online advertising is the second most common way fraudsters reach users online,[4] and they are increasingly using paid for adverts to target users at scale. These adverts can include investment scams, impersonating celebrities and selling fake products.

1.7 The impact of fraudulent advertising is severe. Victims not only lose money, but often suffer emotional distress, and lasting effects on their lives. There are also wider societal and business impacts, as proceeds can fund organised crime and the loss of trust in advertisements undermines legitimate businesses. These impacts can damage communities, distort markets and disproportionately affect smaller firms.

1.8 Organisations and individuals across society need to come together to tackle this harm. Businesses, law enforcement, regulators, civil society, and campaigners all have vital roles to play in tackling online fraudulent advertising.

1.9 The largest online platforms, where most users are present and which often rely on advertising for a large proportion of their revenue, will be central to combatting fraudulent advertising. They need to up their game, providing a better service for their users by

[1] IAB UK, 2026. Digital Adspend 2025: UK's digital ad market reaches £40.5bn. [accessed 22 June 2026].
[2] In effect, the Category 1 and 2A threshold conditions, as set out in secondary legislation, will cover the most widely used services. See the Online Safety Act 2023 (Category 1, Category 2A and Category 2B Threshold Conditions) Regulations 2025; and the OSA Impact assessment, paragraph 80. We have published our 2026 register of categorised services.
[3] Home Office, 2026. Economic and social cost of fraud 2023 to 2024. [accessed 21 April 2026].
[4] The most common method is via a targeted message to the user.

directing more leadership attention and investment to addressing the problem of fraudulent advertising.

1.10 The draft fraudulent advertising code we are consulting on today sets out the steps Ofcom thinks platforms should take to combat fraudulent advertising. Our proposals focus in particular on the following areas:

- **Assess risk and have robust governance processes:** we are proposing that platforms should undertake a 'fraud indicator assessment' to assess how fraudulent advertising manifests on their service and what indicators suggest that individual advertisements and accounts pose a material risk of fraud. They should use these insights to more effectively apply mitigations to tackle this harm. We are also proposing a suite of governance measures so that services' most senior governance bodies have oversight and proper accountability for compliance with their fraudulent advertising duties.
- **Making it harder for fraudsters to access advertising accounts**: we want to make it harder for fraudsters to open and operate advertising accounts. We are proposing a number of measures which will help achieve this objective. Most notably we are proposing that platforms should:
  - Undertake robust checks when advertisers open accounts to check they work for who they say they do;
  - Check advertising accounts for indicators that they are likely to engage in fraud;
  - Do checks to ensure that anyone posting an advertisement for financial services products is legally permitted to do so;
  - Put in place robust security measures to stop bad actors from taking over legitimate advertisers' accounts; and
  - Ban advertisers that post fraudulent advertisements and prevent them from returning to the service.
- **Robust testing of AI tools**: the use of generative AI has significantly reduced the friction and cost associated with producing fraudulent advertisements. To address this, we are proposing that platforms that make AI ad generation tools available to advertisers product test these tools to identify vulnerabilities in them and take steps to address the vulnerabilities they identify.
- **Strengthening reporting functions:** effective reporting is crucial to capturing fraudulent advertising that has evaded detection by other means. We are proposing providers establish a dedicated reporting channel, which enables organisations with the requisite expertise to report fraudulent advertisements quickly and easily. We are further strengthening this, and user reporting, by proposing access to an ad library that has the principles, functionalities and information categories needed to enable experts to quickly identify fraudulent advertising, so it can be taken down.

1.11 We also intend to propose that platforms should use **proactive technology** to detect fraudulent advertising. We will consult on the detail of this proposal in autumn 2026 once we have set out our overall approach to proactive technology detection in our Statement on the current Additional Safety Measures consultation.[5]

[5] We are currently analysing consultation responses to our proposals on proactive technology for UGC content. We intend to publish our statement on this work in autumn 2026.

1.12 The package as a whole represents a layered approach, building in safety by design. Our proposed measures on account checks, the testing of AI tools, the fraud indicator assessment, and our suite of governance measures, all push the platforms to take a more stringent approach to service design to better protect their users.

1.13 In an adversarial context, where platform mitigations are quickly met with counter measures from fraudsters, we consider that our proposed measures would plug important gaps and raise industry standards. There are no major platforms that have all our proposals in place currently.

1.14 Though we think the cost of implementing the package could be substantial, the scale of harm suffered by individuals and the economy means we consider the costs to be worth it. Applying these proposed measures, including our proposals on proactive technology, would make platforms better able to detect and remove fraudulent advertising content and accounts. This should make a material contribution to efforts to combat fraudulent advertising and deliver substantial economic and societal benefits.

Next steps

1.15 We want to extend our thanks to stakeholders for their engagement to date, as we have built up our policy proposals, in particular to those who responded to our Call for Evidence, formal and informal information requests, engaged with our research, and more generally those who have given up some of their valuable time to talk to us about fraudulent advertising.

1.16 Welcome stakeholder feedback via our online response form.

1.17 We have published various accessible materials, including a 'Summary of each section', 'Summary of our proposals', and, a 'Summary of reports, complaints and appeals' to help stakeholders engage with the consultation.

1.18 Our Consultation will close on 2 October. We will consider responses when reaching decisions.

1.19 We plan to publish our Statement by mid-2027 at the latest. Our full regulatory roadmap and strategy is available on our website.

2. Introduction

What is this section of the consultation about?

This section provides a high-level introduction to our Fraudulent Advertising Codes Consultation. It outlines the statutory basis of Ofcom's role, our specific duties in relation to online safety and fraudulent advertising and explains how to navigate this document. To help improve the accessibility of this document we have included suggestions for which parts of our consultation different types of stakeholders might find most useful.

2.1 This section provides a high-level introduction to our consultation on how we propose to give effect to the fraudulent advertising duties and our related enforcement powers (Fraudulent Advertising Consultation) under the Online Safety Act 2023 (the Act).

2.2 This consultation forms part of our wider work to implement an online safety regulatory framework established by the Act. We published our Illegal Content Codes of Practice in December 2024 and our Protection of Children Codes of Practice in April 2025, which are now in force. In our June 2025 Additional Safety Measures Consultation (our June 2025 Consultation), we also consulted on additional safety measures to further strengthen our Illegal Content Codes and Protection of Children Codes.[6] Alongside this Fraudulent Advertising Consultation, we are publishing a separate consultation on additional duties that apply to Category 1 services and our statement on categorisation.[7]

Ofcom's duties and online safety functions

2.3 This sub-section provides a high-level summary of Ofcom's general duties and online safety functions. A full summary of the legal framework for this consultation is set out in Annex 2, 'Legal framework'.

Ofcom's general duties under the Communications Act 2003

2.4 Ofcom is the independent regulator for communications services in the UK. We have regulatory responsibilities for the telecommunications, post and broadcasting sectors, as well as for online services. As a public authority, Ofcom must act lawfully, rationally and fairly.

2.5 The Communications Act 2003 (the 2003 Act) places duties on us that we must fulfil when exercising our regulatory functions, including our online safety functions. The 2003 Act states that our principal duty in carrying out our functions is:

- to further the interests of citizens in relation to communication matters; and
- to further the interests of consumers in relevant markets, where appropriate by promoting competition.[8]

[6] Ofcom, 2025. Additional Safety Measures.
[7] 2026 Additional Duties Consultation and Ofcom's 2026 register of categorised services.
[8] Section 3(1) of the 2003 Act.

2.6 In performing that principal duty, we must have regard to principles set out in the 2003 Act, which says that regulatory activities should be transparent, accountable, proportionate, consistent and targeted only at cases where action is needed.[9]

2.7 When performing our duties, we must ensure that UK citizens are adequately protected from harm caused by content on regulated services through the use by providers of systems and processes designed to reduce the risk of such harm.[10]

2.8 The 2003 Act further requires[11] that we must have regard to the following factors as they appear to us to be relevant in the circumstances.[12] In making our decisions, we have considered factors including, but not limited to:

- the risk of harm to UK citizens presented by regulated services;
- the need for a higher level of protection for children than for adults;
- the need for it to be clear to providers of regulated services how they may comply with their duties under the Act;
- the need to exercise our functions to secure that providers may comply with such duties by taking or using measures, systems or processes which are proportionate to the size or capacity of the provider and the level of risk (and potential severity) of harm presented by the service;
- the desirability of promoting the use of technologies which are designed to reduce the risk of harm to citizens; and
- the extent to which providers demonstrate, in a way that is transparent and accountable, that they are complying with their duties.

2.9 In line with our additional duties under the 2003 Act,[13] we have also considered:

- the desirability of promoting competition and encouraging investment and innovation in relevant markets;
- the vulnerability of children and of others whose circumstances put them in need of special protection;
- the needs of disabled people, older people and of those on low incomes;
- the opinions of consumers and of members of the public generally;
- the interests of persons in the different parts of the UK; and
- the interests of the different ethnic communities within the UK.

The Online Safety Act 2023

2.10 The Act is a set of laws designed to protect children and adults online. It places a range of duties on providers of user-to-user and search services, giving them more responsibility for their UK users' safety. We set out types of services in scope of the Act in our December 2024 Statement on Protecting People from Illegal Harms Online.[14] The Act imposes duties on providers to identify, mitigate and manage the risk of harm from illegal content and

[9] We must also have regard to any other principles appearing to us to represent best regulatory practice.
[10] Section 3(2)(g) of the 2003 Act.
[11] Section 3(4A) of the 2003 Act.
[12] In relation to matters to which section 3(2)(g) is relevant.
[13] Section 3(4) of the 2003 Act.
[14] See 'Overview of regulated services' in Ofcom, 2024. December 2024 Statement on Protecting People from Illegal Harms Online.

activity, as well as content and activity that is harmful to children. It also imposes additional duties on providers of categorised services covering a range of issues, as explained in paragraphs 2.14 to 2.17 in this section.

2.11 The Act establishes Ofcom as the regulator responsible for online safety. It places a requirement on us to prepare and issue Codes of Practice and produce guidance to assist providers in complying with their duties. The duties in the Act only apply to services with links to the UK.[15] They also only apply to the design, operation and use of the service in the UK, or (where the duties relate to users of a service) the design, operation and use of the service as it affects UK users.[16] Consistent with this, we can only make recommendations which relate to the design or operation of a service in the UK or as it affects UK users of the service.[17]

2.12 Our December 2024 Statement on Protecting People from Illegal Harms Online[18] and our April 2025 Statement on Protecting Children from Harms Online[19] set out the package of guidance and Codes measures that we recommend providers adopt to comply with their duties relating to illegal content and protection of children under the Act. Our June 2025 Consultation also consulted on additional safety measures to further strengthen our Illegal Content Codes and Protection of Children Codes.[20]

2.13 This consultation proposes Fraudulent Advertising Codes of Practice measures that we recommend providers adopt to comply with their fraudulent advertising duties discussed further in paragraphs 2.18 to 2.26.

Duties on providers of Category 1 and Category 2A services

2.14 The Act establishes categories of regulated user-to-user and search services which are subject to additional requirements. Category 1 and Category 2B relate to different kinds of regulated user-to-user services, with Category 1 being the largest services. Category 2A relates to search services. The Secretary of State is responsible for setting threshold conditions for these categories based on the number of users of the service, its functionalities and other relevant factors.[21]

2.15 We have today published the register of categorised services.[22] Services listed on the register must comply with additional duties. These duties include giving users more tools to control what content they see, ensuring protections for news publisher and journalistic content, preventing fraudulent advertising (which is the subject of this consultation), and producing transparency reports. The specific duties vary depending on the category of the service. The Act requires us to produce Codes of Practice and guidance outlining the steps that providers can take to comply with these additional duties.

---

[15] This is defined in section 4 of the Act for user-to-user and search services, and in section 80 of the Act for services on which regulated provider pornographic content is displayed. Such services must also not be exempt under Schedules 1 or 9 to the Act.
[16] Section 8(3) of the Act.
[17] Paragraph 11 of Schedule 4 to the Act.
[18] Ofcom, 2024. December 2024 Statement on Protecting People from Illegal Harms Online.
[19] Ofcom, 2025. April 2025 Statement on Protecting Children from Harms Online.
[20] Ofcom, 2025. Additional Safety Measures.
[21] Schedule 11 of the Act. These are set out in The Online Safety Act 2023 (Category 1, Category 2A and Category 2B Threshold Conditions) Regulations 2025.
[22] Ofcom's 2026 register of categorised services.

2.16 In December 2025 we published draft guidance on the deceased child user duties which apply to regulated user-to-user services, search services and combined services with links to the UK that are listed on the register of categorised services.[23]

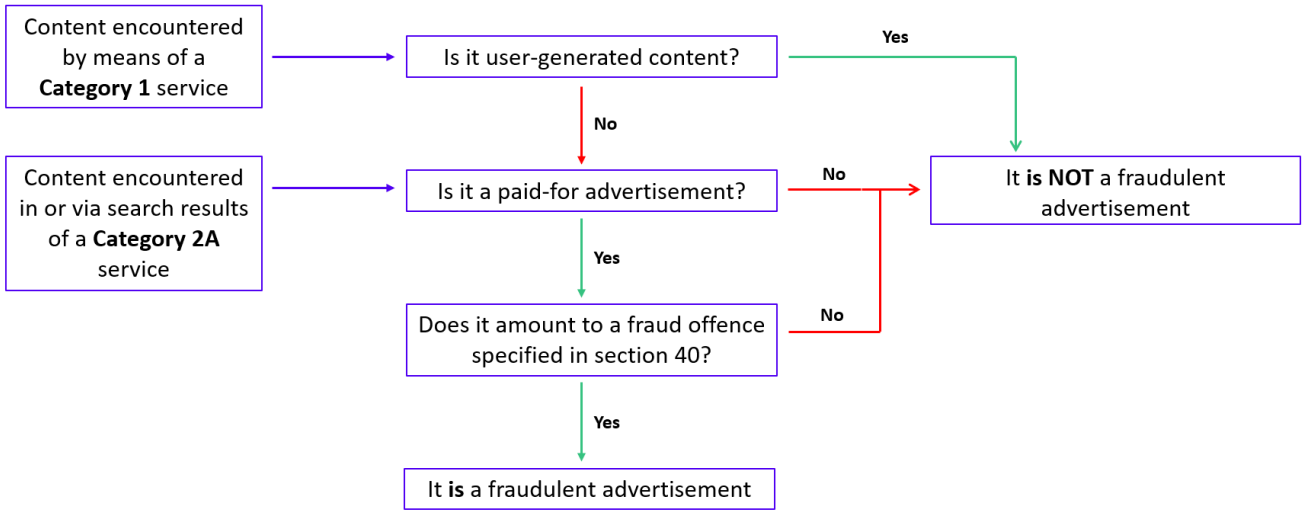
2.17 We have also published a consultation on additional duties for Category 1 services. This includes duties related to user empowerment; optional user identity verification; protections for news publisher and journalistic content and content of democratic importance; freedom of expression and privacy impact assessments; and additional terms of service and complaints.

Fraudulent advertising duties

2.18 The focus of this consultation is on the fraudulent advertising duties which apply to providers of Category 1 and 2A services.

2.19 In relation to a Category 1 or 2A service, an advertisement is a 'fraudulent advertisement' if it is a paid-for advertisement, which we explain in paragraph 2.20,[24] it amounts to an offence specified in section 40, and (for Category 1 services) it is not regulated user-generated content.[25] Figure 2.1 sets this out in more detail.[26]

Figure 2.1: Flowchart showing how to decide if content is a fraudulent advertisement



[23] Ofcom, 2025. Consultation: Guidance – Deceased Child User Duties.
[24] Defined in section 236 of the Act.
[25] Sections 38(3) and 39(3) of the Act. 'Regulated user-generated content' is defined in section 55 of the Act.
[26] For Category 2A services, section 39 of the Act explains that 'in or via search results' refers to encountering fraudulent advertisements (i) in search results of the service, or (ii) as a result of interacting with a paid-for advertisement in search results of the service (for example, by clicking on it). It does not include references to encountering fraudulent advertisements as a result of any subsequent interactions with an internet service other than the search service.

2.20 For an advertisement to be a paid-for advertisement, the service provider must be paid[27] to display it,[28] and there must be a contractual arrangement[29] between the service and the party placing the advertisement, which determines the placement of the advertisement.[30]

2.21 Section 40 of the Act sets out the various offences for when an advertisement is considered fraudulent. This includes financial services offences, general fraud offences and offences in relation to false or misleading information about financial markets. We are consulting on draft guidance to assist providers in determining whether an advertisement is fraudulent.[31]

2.22 Paid-for advertisements typically include a 'click-through', such as a URL that directs users to an external webpage (landing page) where users are encouraged to take further action. On Category 2A search services, these landing pages are considered part of the paid-for advertisement when encountered as a result of a single interaction with the advertisement in search results (such as by clicking on it). Webpages encountered as a result of any subsequent interactions are not considered part of the paid-for advertisement. Across both service types, information about the destination of an advertisement (including landing pages) may constitute relevant and reasonably available information that providers can take into account when assessing whether an advertisement is fraudulent, depending on the circumstances.

2.23 The Act places a duty on providers of Category 1 services to use proportionate systems and processes designed to:

- prevent individuals from encountering content consisting of fraudulent advertisements by means of the service;
- minimise the length of time for which such content is present; and
- where the provider is alerted by a person to the presence of such content, or becomes aware of it in any other way, swiftly take down such content.[32]

2.24 Providers of Category 2A services have a duty to use proportionate systems and processes designed to:

- prevent individuals from encountering content consisting of fraudulent advertisements in or via search results of the service;
- if any such content may be encountered in or via search results of the service, minimise the length of time that is the case; and
- where the provider is alerted by a person to the fact that such content may be so encountered, or becomes aware of that fact in any other way, swiftly ensure that individuals are no longer able to encounter such content in or via search results of the service.[33]

[27] Or receive some other non-monetary consideration.
[28] Payment may be directly from the advertiser or indirectly from another person.
[29] A contractual arrangement may be created in a variety of ways, including through the acceptance of terms of service or equivalent provisions.
[30] This definition appears in section 236 of the Act.
[31] See Annex 9, 'Guidance on making fraudulent adverting judgement: updates to the Illegal Content Judgements Guidance'.
[32] Section 38(1) of the Act.
[33] Section 39(1) of the Act.

2.25 We refer to the duties in paragraphs 2.23 to 2.24 as the 'fraudulent advertising duties'. When determining what is proportionate, the Act specifies that certain matters are particularly relevant. They are:

a) the nature and severity of potential harm to individuals presented by different kinds of fraudulent advertisement; and
b) the degree of control the service provider has in relation to the placement of advertisements on the service.[34]

2.26 Category 1 and 2A service providers must also include clear and accessible provisions in their terms and statements giving information about any proactive technology used by the service to comply with the fraudulent advertising duties[35] (including the kind of technology, when it is used and how it works). We refer to the duties in respect of the terms and statements as the fraudulent advertising (terms of service) duties.[36]

Growth duty

2.27 Ofcom is required, when exercising our regulatory functions, to have regard to the desirability of promoting economic growth, including by ensuring that the regulatory action we take is necessary and proportionate.[37] This duty is referred to as the 'growth duty', which has applied to our online safety function since 6 April 2026.

2.28 We are also required to have regard to the government's statutory guidance on the growth duty.[38] That guidance explains that the duty needs to be considered alongside our other statutory duties, and that its purpose is not to achieve or pursue economic growth at the expense of necessary protections.[39] Among other things, it also identifies particular drivers of economic growth, including innovation, investment and competition.

2.29 We comply with this duty by considering the wider economic impacts of our proposals in our Combined Impact Assessment in Volume 1, Section 6, 'Other relevant considerations'.

Government's strategic priorities

2.30 Ofcom must have regard to the government's priorities for online safety when carrying out our online safety functions, as set out in section 92 of the Act.

2.31 The UK Government's Statement of Strategic Priorities (SSP) for online safety was designated on 2 July 2025.[40] We published our response on 25 July 2025, in which we set out the work we planned to carry out in the coming year that is relevant to the priorities set out in the SSP.[41] In particular, in relation to the priority about "inclusivity and resilience", we highlighted that we would be considering risks associated with deepfake fraudulent

[34] Sections 38(5) and 39(6) of the Act. Throughout this consultation we refer to providers 'placing' advertisements. This reflects the Act which refers to the degree of control the service provider has in relation to the placement of advertisements.
[35] Set out at sections 38(1) or 39(1) of the Act (as applicable).
[36] Set out at sections 38(2) or 39(2) of the Act (as applicable).
[37] Section 108 of the Deregulation Act 2015.
[38] Section 110(3) of the Deregulation Act 2015.
[39] Department for Business and Trade, 2024. Growth Duty – Statutory Guidance. [accessed 18 June 2026].
[40] Department for Science, Innovation and Technology, 2025. Statement of Strategic Priorities for Online Safety. [accessed 26 June 2026].
[41] Ofcom (Davies, K.), 2025. Letter to Government on the Statement of Strategic Priorities for Online Safety.

advertising and how they can be tackled as part of our consultation on the Fraudulent Advertising Codes.[42]

Equality legislation and Welsh language

2.32 We considered the equality impacts of our proposals, detailing our understanding of any particular impacts on persons with protected characteristics and other relevant groups in the UK.

2.33 Where relevant, and to the extent we have discretion to do so in the exercise of our functions, we consider the potential impacts on opportunities to use the Welsh language and the need to treat the Welsh language no less favourably than English (in accordance with Welsh language standards).

2.34 We have set out our considerations on these matters in Annex 6, 'Equality Impact Assessment and Welsh Language Impact Assessment'.

How to use and navigate this document

2.35 It is important that the set of documents that form this consultation are accessible and clear to navigate for a range of audiences. We have responded to feedback received from previous consultations published as part of Ofcom's duties under the Act and have taken steps to improve accessibility and navigation.

2.36 For this consultation we have produced the following accessible materials:

- A summary of our proposals, which include a summary of our draft Fraudulent Advertising Codes of Practice and which providers they apply to.
- A summary of each section, which set out what each section is about, why we have made the proposals, and our consultation questions.
- Summary of reports, complaints and appeals, which detail the different user journeys via flowcharts.

2.37 We will also engage with relevant stakeholders following the publication of this consultation.

2.38 We are aware that different stakeholders reading this consultation will have different priorities, and therefore may be interested in different parts of the consultation. We have also taken into account that civil society organisations and interested individuals are likely to have less time and resource to engage with our proposals.

2.39 We have set out our views (numbered i to iv) of which elements of our overall consultation package might be of most use to different kinds of stakeholders.

i) **Civil society organisations**: may be particularly interested in the reasoning for our proposals, starting with our 'Overview' and summary of each section document. They may identify areas of specific interest to read in more detail, such as the 'Causes and impacts of fraudulent advertising' in Volume 1, Section 4 or the full section on any particular measure in Volumes 2 to 4.

[42] In this regard, see Volume 1, Section 4, 'Causes and impacts of fraudulent advertising' where we set out relevant evidence relating to the impacts of AI-generated fraudulent advertising (also referred to as 'deepfakes').

ii) **Category 1 or Category 2A service providers**: will most likely want to review the full range of materials. We would expect their focus to be on the proposals in Volumes 2 to 4 and the draft Codes documents in Annexes 4 and 5.

iii) **Individuals within service providers**:

a) Compliance lawyers may want to focus initially on our draft Codes documents.

b) Trust and safety workers may want to focus on Volume 1, Section 4, 'Causes and impacts of fraudulent advertising'; Volume 4, Section 2, 'Advertising moderation'; the draft Codes; and our updates to the Illegal Content Judgements Guidance in Annexes 9 to 11. We note that these are proposals at this stage, and therefore it would be most useful to review these same documents again when we publish our Fraudulent Advertising Statement.

iv) **Individuals who have a broader interest in online safety / fraud**: might wish to begin with our 'Overview' section, as well as potentially the summary of our proposals and summary of each section documents.

2.40 Our consultation on the fraudulent advertising duties is broken down into **four volumes**. **Our first volume** contains our **overview** and **context documents**, then **Volumes 2 to 4** set out our **proposed measures with our reasoning**. We then provide a number of **Annexes**, which include our **regulatory documents** and our **glossary**.

2.41 Within **Volume 1**, our overview gives a high-level summary of our proposals, how we think they would address fraudulent advertising, and next steps. In it, we note the importance of organisations and individuals from across all sectors coming together to tackle this egregious harm. The volume comprises:

- Section 1: Overview;
- Section 2: Introduction (this document);
- Section 3: Online advertising ecosystem;
- Section 4: Causes and impacts of fraudulent advertising;
- Section 5: Approach to Codes; and
- Section 6: Combined impact assessment.

2.42 **Volume 2, Risk, governance and control**, sets out our proposals on how providers can more effectively identify material risks on their services, and seek to mitigate them effectively and proportionately. In particular, our governance proposals aim to ensure there would be senior oversight and accountability for the implementation and operation of the measures set out in the Codes. The volume comprises:

- Section 1: Introduction;
- Section 2: Advertising intermediaries;
- Section 3: Fraud indicator assessment;
- Section 4: Governance and accountability; and
- Section 5: Testing advertisement generation tools.

2.43 **Volume 3, Ensuring account integrity**, explains our proposals designed to raise the bar on account integrity. Specifically, we are proposing a range of measures to better ensure service providers take sufficiently robust steps to check that advertising account holders opening and operating accounts are not bad actors, that when bad actors are identified

they receive an appropriate ban, and that legitimate advertising account holders can quickly and easily report suspected account takeover. The volume comprises:

- Section 1: Introduction;
- Section 2: Account checks and actions;
- Section 3: Preventing fraudulent financial services advertising;
- Section 4: Countering account takeover;
- Section 5: Advertising bans; and
- Section 6: Account appeals.

2.44 **Volume 4, Moderation**, sets out our proposals around moderation, reporting, complaints and appeals. Though it is crucial that services are designed in a way that reduces harms to users, it is not possible to entirely prevent fraudulent advertising through these mitigations alone. Therefore, it is important for service providers to have effective moderation and reporting tools that can help to identify fraudulent advertisements, so that they can be taken down quickly. The volume comprises:

- Section 1: Introduction;
- Section 2: Advertising moderation;
- Section 3: Terms of service and publicly available statements;
- Section 4: Advertising complaints; and
- Section 5: Ad libraries.

2.45 We have eleven **Annexes**, including two regulatory documents (Annexes 4 and 5) and three guidance documents (Annexes 9 to 11). We expect, once finalised, service providers will use these to ensure compliance with the fraudulent advertising duties:

- Annex 1: Stakeholder responses;
- Annex 2: Legal framework;
- Annex 3: Statutory tests;
- Annex 4: Draft Code of Practice for Category 1 services;
- Annex 5: Draft Code of Practice for Category 2A services;
- Annex 6: Equality Impact Assessment and Welsh Language Impact Assessment;
- Annex 7: Glossary;
- Annex 8: Further detail on economic assumptions and analysis;
- Annex 9: Guidance on making fraudulent adverting judgement: updates to the Illegal Content Judgements Guidance;
- Annex 10: Draft amendments to the Illegal Content Judgement Guidance- Chapter 1; and
- Annex 11: Draft annex to ICJG – Guidance on fraudulent advertising judgements.

3. Online advertising ecosystem

What is this section about?

This section presents a generalised understanding of the online advertising ecosystem, and the ways providers can place paid-for advertisements on Category 1 and 2A services.

Online advertising uses data and technology to facilitate personalised advertising. Both search and display advertising use bidding and auction infrastructure: search advertising is traded through a keyword-based auction, while display advertising is placed on services via technological systems and functions known as 'adtech'. The functions involved in these systems form part of the 'advertising supply chain', which we refer to as an 'advertising pathway'. An advertisement will travel through a particular advertising pathway to get from the advertiser (or media agency) to the service it is to be placed on.

Providers can use different types of advertising pathways (either exclusively or in combination) to place advertisements on their service:

a) They can use a system where the supply chain is 'owned and operated' by or integrated with the service (sometimes described as a 'walled garden').

b) They can use the open-display market, where advertisements, ad slots and ad impressions are sold and bought using a range of advertising intermediaries.

c) We also note that providers can engage in 'direct deals' (either within an owned-and-operated supply chain or through the open-display market), where the provider enters into a direct agreement with an advertiser to place advertisements from their business on its service(s).

Advertising pathways or supply chains are complex and dynamic, often varying between services. An owned-and-operated supply chain is a complex **centralised** system. An open-display supply chain is a complex and dynamic **decentralised** system.

The pathway a provider uses to place advertisements on its service – and the level of integration of parts of the supply chain within the service – has an impact on decisions providers make related to the placement of advertisements on a service, and any mitigations against fraudulent advertising.

Consultation question

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

Introduction

3.1 This section sets out our understanding of the online advertising ecosystem and the advertising pathways that providers of Category 1 and Category 2A services may use to place paid-for advertisements on their services.

3.2 We start the section with an overview of regulated services, paid-for advertisements as defined in the Online Safety Act 2023 (the Act) and the online advertising sector.

3.3 We then set out our understanding of advertising pathways, which relates to the different journeys an advertisement can take to be placed on a service. Our understanding of these pathways comes from industry research and reports, and from our own analysis.

Regulated services, paid-for advertisements and online advertising

Overview of regulated services

3.4 The Act regulates user-to-user services, search services and combined services, and imposes duties on those services to reduce the risk of harm from illegal content. For an overview of the Act, see Volume 1, Section 2, 'Introduction', paragraph 2.10 to 2.13.

3.5 The Act places additional duties on a subset of providers of regulated services which meet certain conditions to be 'categorised'.[43] These include duties to take action in respect of fraudulent advertising.[44]

3.6 While all categorised services within scope of the fraudulent advertising duties will have a significant number of UK users (at least 7 million monthly active UK users), we recognise the diversity and range within this group in relation to the sizes of the services. There is also significant variation within this group of categorised services in relation to the proportion of content on these services that amounts to a paid-for advertisement.

3.7 Fraudulent advertising can have an impact on service providers, which can create incentives for providers (such as increased user and advertiser trust to enhanced service reputation) to address and reduce fraudulent advertising on their services.[45] However, the online advertising market has several interlinked characteristics which mean these incentives may not be strong enough to drive the best safety outcomes for users. Most notably:

- The relevant markets are highly concentrated with limited competition. This is particularly the case for categorised services, where there are a smaller number of larger services. A 2020 market study from the Competition & Markets Authority (CMA) found that Google and Meta account for the majority of the search and display advertising market in the UK.[46] High concentration and limited competition could reduce incentives for providers to prioritise safety outcomes because of their strong market positions.
- The costs and negative impact of fraudulent advertising primarily affect users who are misled by such advertisements, rather than the service providers. Less fraudulent advertising generally means fewer advertisements overall, which means less revenue for the provider. This means that providers have weak incentives to address fraudulent advertising. Evidence from the Integrity Institute highlighted that there were few consequences from fraudulent advertisements because services could avoid the penalties (such as 'chargebacks') which come from connecting customers to fraudulent experiences.[47]

---

[43] For more information on categorisation, see Volume 1, Section 2, 'Introduction', paragraphs 2.14 to 2.17.
[44] See Volume 1, Section 2, 'Introduction', paragraphs 2.18 to 2.26 for an explanation of the fraudulent advertising duties. See Volume 1, Section 4, 'Causes and impacts of fraudulent advertising' for an overview of what fraudulent advertising is and how it manifests.
[45] For more on detail on the impacts of fraudulent advertising, see Volume 1, Section 4, 'Causes and impacts of fraudulent advertising'.
[46] CMA, 2020. Online platforms and digital advertising: market study final report, p.5. [accessed 22 June 2026].
[47] 'Chargebacks' are fees that payment processers apply to a business for any disputed purchases. In general, chargebacks help ensure that businesses provide a level of service and quality that meets customer expectations. For online services selling advertising, chargebacks only apply if an advertiser disputes the cost of advertising. Source: Ofcom and Integrity Institute, 2026. Fraudulent advertising and account integrity: Expert insights on best practice.

- Similarly, actions designed to prevent fraudulent advertising often introduce friction into the process of buying and selling advertising space on services, and result in costs for providers. This can reduce profitability, diluting providers' incentives to put in place mitigations.[48]
- Service providers – and relevant markets more broadly – are perhaps more incentivised and motivated to deal with ad fraud instead of fraudulent advertising. This is because ad fraud is generally considered to affect the advertising industry and revenue for advertisers, rather than end users. For more on the differences between ad fraud (also known as 'click fraud') and fraudulent advertising, see Volume 1, Section 4, 'Causes and impact of fraudulent advertising', paragraph 4.7.
- There are informational asymmetries in how the online advertising ecosystem operates, particularly in the open-display market. The ecosystem relies on a range of intermediaries (which are actors within advertising supply chains that are involved in the automatic buying, selling and serving of online advertisements), and vast amounts of data flows, but service providers do not always know who those actors are and what information is being shared. This can make safety-focused interventions difficult. A 2022 Beruku and Which? report highlighted that the nature of the digital advertising supply chain makes the open-display market opaque: the lack of transparency makes exploitation easier.[49]

3.8 The Act is intended to improve online safety for UK users. This includes having proportionate systems and processes designed to prevent users from encountering fraudulent advertising. The measures we are proposing to recommend as part of the Fraudulent Advertising Codes will help service providers to take steps that proactively and reactively address fraudulent advertising.[50]

Paid-for advertisements

3.9 The duties relating to fraudulent advertising apply to paid-for advertisements.[51] As described in Volume 1, Section 2, 'Introduction', paragraphs 2.18 to 2.26, a fraudulent advertisement is a paid-for advertisement that amounts to an offence specified in section 40 of the Act. In respect of a Category 1 service only, a fraudulent advertisement cannot be regulated user-generated content (this does not apply to Category 2A services).[52] Therefore, such content is not covered by the fraudulent advertising duties in section 38 of the Act.

3.10 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. We

[48] Reporting from Reuters indicated that fraudulent advertisements could comprise a significant percentage of Meta's annual revenue, based on internal company projections. Source: Horwitz, J., 2025. Meta is earning a fortune on a deluge of fraudulent ads, documents show, Reuters, 6 November. [accessed 22 June 2026]; Ofcom and Integrity Institute, 2026. Fraudulent advertising and account integrity: Expert insights on best practice.

[49] Beruku and Which?, 2022. Fraud in the open-display advertising market, pp.6 to 9. [accessed 22 April 2026].

[50] For more on our approach to developing Codes measures, see Volume 1, Section 5, 'Approach to Codes'.

[51] An advertisement is a 'paid-for advertisement' in relation to an internet service if (a) the provider of the service receives any consideration (monetary or non-monetary) for the advertisement (whether directly from the advertiser or indirectly from another person), and (b) the placement of the advertisement is determined by systems or processes that are agreed between the parties entering into the contract relating to the advertisement. Section 236 of the Act.

[52] Sections 38(3) and 39(3) of the Act.

understand that multiple systems and processes can be involved in placing such content, including systems and processes related to user-generated content.[53]

3.11 User-generated content that appears on a user-to-user service is likely to be subject to the illegal content safety duties and the protection of children duties. Recommended measures for the purposes of complying with these duties are set out in our Illegal Content Codes of Practice and Protection of Children Codes of Practice.[54] In the first instance, it is for a provider of a Category 1 service to determine whether 'boosted' or 'promoted' content on their service is user-generated content. This is likely to depend, among other things, on the systems and processes involved in placing such content. Providers should then determine, accordingly, which duties and Code they should follow in relation to such content.

Overview of the online advertising sector

3.12 Online advertising is the largest advertising medium in the UK: the Advertising Association reported that datasets showed that in 2024 80% of advertising budgets were spent online.[55] UK advertising spend has continued to increase across the board, with social media advertising increasing 21% in 2025.[56] Online advertising is broadly split into two categories, with advertising on these two categories being traded slightly differently:[57]

a) Search advertising is when advertisements are placed on search services based on a user's search query.
b) Display advertising is when advertisements are placed on services alongside or within content.

3.13 The Interactive Advertising Bureau UK (IAB UK) estimated that the UK's digital advertising market surpassed £40.5 billion in 2025, with search advertising accounting for 44% of digital advertising spend.[58] Ofcom's 2024 Online Nation report stated that, in almost all cases, search services made nearly all their revenue from advertising via paid search.[59]

3.14 Online advertising takes many forms. It can include text, images, videos, audio or URLs, and can be static, animated or audiovisual.[60] According to the IAB UK's most recent study, at an estimated £9.3 billion, video advertisements accounted for 23% of digital advertising spend in 2025.[61]

---

[53] We understand that different systems and processes can be involved in placing and paying for content known as boosted content. In some scenarios, a user makes a post, and then subsequently decides to pay the service to increase the circulation and boost it afterwards. In other circumstances, it is possible that a user uses an advertising account and advertising functionalities to create and pay for an advertisement which is presented in the format of a user-generated post.
[54] Ofcom, 2025. Illegal content Codes of Practice for user-to-user services and Illegal content Codes of Practice for search services; Ofcom, 2026. Protection of Children Code of Practice for user-to-user services and Protection of Children Code of Practice for user-to-user services
[55] Advertising Association, 2025. UK Advertising records £42.6bn spend in 2024. [accessed 22 June 2026].
[56] Advertising Association, AA/WARC updates advertising expenditure report to capture evolving UK media landscape and records £46.7bn media investment in 2025. [accessed 25 June 2026].
[57] The CMA generally refers to two forms of advertising, as explained in CMA, 2020. Online platforms and digital advertising, p.6. [accessed 22 June 2026].
[58] IAB UK, 2026. Digital Adspend 2025: UK's digital ad market reaches £40.5bn. [accessed 22 June 2026].
[59] Ofcom, 2024. Online Nation: 2024 Report, p.29.
[60] House of Commons Library (Conway, L.), 2022. Online Advertising Research Briefing, p.9. [accessed 22 June 2026].
[61] IAB UK, 2026. Digital Adspend 2025: UK's digital ad market reaches £40.5bn. [accessed 22 June 2026].

3.15 There are different methods of placing advertisements on a service, and this will differ from service to service depending on decisions around advertisement placement that the provider of each service has made. We refer to these methods as 'advertising pathways' (explained in more detail in paragraphs 3.16 to 3.25) and use that phrase to describe the systems and processes that an advertisement will travel through to get from the advertiser (or a media agency) to the service it is to be placed on. These pathways are also known as 'supply chains'.

What do we mean by 'advertising pathways'?

3.16 Online advertising can be placed on a service in different ways. These methods of placement are dynamic, complex and intricate, and we provide a generalised understanding of two pathways only.

3.17 Broadly, online advertising is placed on services through a series of technological systems and functions known as 'adtech' (sometimes known as 'adtech stack') that are focused on serving an advertiser's content into an ad slot (which is where the advertisement is placed) on a website or an app. Adtech refers to a set of software platforms, infrastructure and data systems that any actor or vendor in an advertising supply chain can use to enable, manage and optimize their role in the buying, selling, delivery and measurement of online advertising. The collective supply of ad slots is often known as 'inventory'. The functions involved in these systems and processes form part of the advertising supply chain.

3.18 An advertising account holder (or media agencies acting on an advertiser's behalf)[62] will post a paid-for advertisement which is stored on the service or by a relevant advertising intermediary until it is placed on the categorised service: [63] this means there is often a gap between when an advertisement is created and when it goes 'live' (when it is encountered by a user).[64]

Advertisers[65] and advertising account holders

3.19 There are different types of advertising accounts that may be involved in the posting of a paid-for advertisement. Generally, we understand that advertising activity operates within a hierarchical structure that can include different types of advertising accounts, such as corporate accounts and individual or manager advertising accounts, which together form an advertising hierarchy.

3.20 Advertising is managed and posted by a range of types of advertising accounts performing different functions depending on how the advertising system is structured on the service. In

[62] Media agencies can exist in both supply chains. When a supply chain is owned-and-operated, the provider will have full transparency over which individuals are acting on behalf of the advertiser. This may not be the case in open-display supply chains.
[63] The categorised service (Category 1 or Category 2A) is the end point where the advertisement is made available (or served) to the user. The categorised service is also often (but not necessarily) the owner and operator of their own adtech systems and processes) required to place an advertisement.
[64] A paid-for advertisement or paid-for financial services advertisement is said to be 'posted' when it has been submitted or uploaded to a service by account holders or account operators to be placed on a service by a provider.
[65] We broadly consider an advertiser to be those who are posting the paid-for advertisement, including advertising account holders and the individual or firm whose products or services are being advertised.

the following list we explain how we are using relevant terms across the consultation. These terms are interlinked and interact with each other in different ways:

a) At the top of the advertising hierarchy is the organisation or brand that ultimately benefits from the advertisements placed.
b) An advertising account holder refers to all persons using an advertising account who are able to post paid-for advertisements. Advertising account holders could operate at a range of levels based on how the advertising system is structured. For example, this could be a 'manager' or 'parent' account representing a brand, or an 'individual' account performing operation actions, such as creating an ad campaign. In some cases, the account holder may also be the individual or organisation being advertised.[66]
c) Advertising can be posted and placed using 'ad manager tools' that are integrated with a service or offered through intermediaries. It can also be placed by media agencies working on behalf of several brands.
d) An advertising account is an account that can post an advertisement.

Functions in an advertising supply chain

3.21 The CMA explains that the process of serving an advertisement on a service to a user generally requires several functions. These are:

a) the creation of an advertisement;
b) the selling of inventory to advertisers;
c) the targeting of advertisements to users;
d) the advertiser's advisory function which determines bidding strategies based on the advertiser's campaign objectives;
e) the publisher's sales function which sets rules for the selling process and determines who inventory is allocated to;
f) the verification and attribution of advertiser campaigns; and
g) the serving of the advertisement to the user.[67]

3.22 These functions occur based on the type of advertising being placed on the service and on the provider's choices about how they organise the sales process on their service. Sometimes, these processes are separate stages within one integrated system where the supply chain is a centralised system (owned-and-operated). Sometimes, these processes happen through a series of connected but separate systems, involving several actors or vendors, where the supply chain is a decentralised system (the open-display market):

a) In owned-and-operated systems (sometimes known as a 'walled garden'), the service provider has integrated the advertising supply chain within the service. The service provider can determine which advertisers can advertise on the service, the advertisements that are placed on the service, and the process to decide which advertisement is served to a user. Figure 3.1 presents a simplified version of an owned-and-operated supply chain.
b) In the open-display market, advertising inventory is sold and bought using advertising intermediaries. The CMA explains that there are two routes through which this can happen: (i) the provider can sell inventory on its service through an ad network of an

[66] An advertiser might use an advertising agent. An agent is a business (or individual) that plans, creates and/or manages digital marketing campaigns across online services. A business or individual with a product or service to promote may engage an agent to submit advertisements to relevant online services.
[67] CMA, 2020. Online platforms and digital advertising, p.219. [accessed 22 June 2026].

owned-and-operated platform, or (ii) the provider can sell inventory on its service through advertising intermediaries.[68] The service provider may have a role in determining which types of advertisements are placed on the service (see paragraph 3.38). Figure 3.2 presents a simplified version of an open-display supply chain.

3.23 Generally, with display advertising, the process of matching advertisements to users on services is known as 'programmatic advertising'. This is automated advertising, which looks different depending on the advertising pathway a service uses or the level of integration of the advertising supply chain with a service.

a) In some cases, programmatic advertising can be facilitated by a real-time bidding (RTB) process that involves advertisers (or agencies acting on behalf of an advertiser) and a service's 'publisher ad server'. In the RTB process, actors or vendors within the supply chain use data to decide which advertisement should be placed on a service and served to a particular user.[69] These auctions allow advertisers (or media agencies acting on their behalf) to bid for an ad impression, and services (or intermediaries acting on their behalf) to decide which advertisement to place.[70]
b) Automated advertising can also be done without an auction process. In some instances, a service can partner directly with an individual supply-side platform (explained in paragraph 3.32), or they can engage in private marketplaces.
c) Where the supply chain is integrated with the service (see paragraph 3.26), the auction process is proprietary and advertisers generally bid on a variety of outcomes in addition to impressions.

3.24 Search advertising refers to paid-for advertisements on search services. It is generally based on keyword searches to ensure that the advertisement that is placed on a search service aligns with the user's search query. Generally, advertisements that appear on search services are ranked: the ranking of an advertisement often determines how much organisations or brands have to pay for advertising on search services. Typically, an advertiser will pay if and when a user clicks on their advertisement.[71]

3.25 Our initial analysis of advertising pathways suggests that some of the largest providers of categorised services will sometimes use a combination of pathways to place advertisements on their services.[72] Conversely, advertisers will also use a combination of pathways to reach users.[73] We explain in Volume 1, Section 5, 'Approach to codes', how these different pathways might affect the application of our proposed measures.

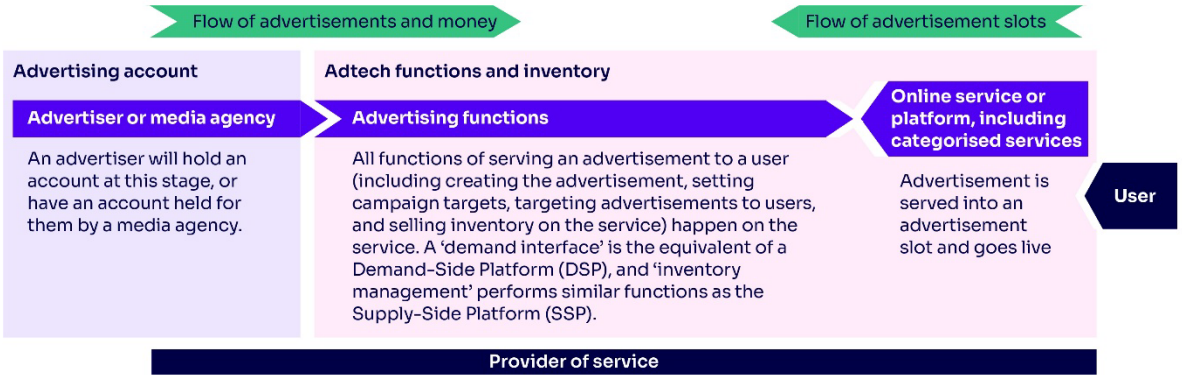
---

[68] CMA, 2020. Online platforms and digital advertising, p.220. [accessed 22 June 2026].
[69] House of Commons Library (Conway, L.), 2022. Online Advertising Research Briefing, pp.14 and 15 [accessed 22 June 2026].
[70] CMA, 2020. Online platforms and digital advertising, p.221. [accessed 22 June 2026].
[71] For more on how search advertising works, see Avenga, 2025. What is search advertising and how does it work?. [accessed 22 June 2026].
[72] We know from responses to our formal requests for information that some categorised services generate revenue from ads placed through advertising intermediaries. In some cases ([✂] and [✂]), a small percentage of revenue from advertisements is derived from advertisements served through intermediaries. In other cases ([✂]), a percentage of revenue from advertisements is derived from advertisements served through intermediaries. Sources: [✂] response to our formal information request issued 26 June 2025; [✂] response to our formal information request issued 26 June 2025.
[73] House of Commons Library (Conway, L.), 2022. Online Advertising Research Briefing, p.11. [accessed 22 June 2026].

Owned-and-operated supply chains

3.26 A walled garden is a "closed ecosystem in which a platform provides a complete end-to-end technical solution for advertisers and publishers".[74] The functions necessary to the placement of paid-for advertisements are part of a vertically integrated supply chain, also known as an 'owned-and-operated' supply chain.[75] The supply chain is 'vertically integrated' because the functions of the supply chain are handled by the service provider itself rather than by separate actors in the market: the service provider owns the advertisement inventory, the tools to buy advertising space and the data required to place advertisements, and it controls the auction process that determines which advertisements are served to users.[76]

Figure 3.1: Simplified diagram of an owned-and-operated supply chain.[77]



Where relevant, we have used terms familiar to the advertising industry to describe the supply chain. At the end of the supply chain, we use terminology consistent with the Online Safety regime. 'Provider', 'categorised service' and 'user' are terms consistent with the Online Safety Act.

Applying measures in an owned-and-operated supply chain

3.27 When a supply chain is owned-and-operated, service providers would generally have an active role over all aspects of the advertising supply chain. This is because of the vertical integration of the adtech functions, which means that service providers handle the requisite functions to place an advertisement on the service. This means that they are able to apply safety measures across that supply chain. For example, this would mean that:

- The provider knows which advertising account holders want to post advertisements on its service(s), so it can verify those advertisers and run account checks.

---

[74] CMA, 2020. Online platforms and digital advertising, p.155. [accessed 22 June 2026].
[75] SparkNinety, 2022. Online advertising programme market insights: final report, p.41. [accessed 22 June 2026].
[76] There are variations of owned-and-operated supply chains. In some cases, adtech functions are wholly integrated with the service; in other cases, adtech functions can be shared across a number of a provider's (or their parent company's) services. We also note that open-display supply chains can feature some vertical integration. Source: SparkNinety, 2022. Online advertising programme market insights: final report, p.9. [accessed 22 June 2026].
[77] This simplified diagram draws from a similar diagram produced by SparkNinety (for the UK Department of Culture, Media and Sport). The diagram has been adapted to show key concepts relating to the Act and the Fraudulent Advertising duties. Source: SparkNinety, 2022. Online advertising programme market insights: final report, p.41. [accessed 22 June 2026].

- The provider can see advertisements before they are live on the service, so can moderate them before they are placed on the service. Because providers can see the advertisement and associate it to an advertising account, they will also have the ability to moderate and take appropriate action in respect of complaints about suspected fraudulent advertisements.

3.28 In some circumstances, service providers can use advertising intermediaries to perform some of the functions in an owned-and-operated supply chain. These intermediaries could be integrated in the owned-and-operated supply chain. Due to the integration of these intermediaries, the service provider is able to play an active role in the application of measures in these circumstances.

Open-display supply chains

3.29 Service providers can also use a supply chain that is not owned-and-operated by them to place advertisements on their services. An open-display supply chain consists of adtech functions provided by a range of advertising intermediaries between an advertiser and the services upon which an advertisement is placed.[78] These adtech functions connect advertiser demand with a service's supply of advertising inventory.

3.30 The following actors or functions are involved on the demand side, generally representing the advertiser (this is a non-exhaustive list):

a) advertisers or media agencies acting on behalf of advertisers;
b) advertiser ad servers where advertisements are stored; and
c) demand-side platforms (DSPs) that allow advertisers and media agencies to buy inventory. A DSP will bid on impressions for the advertiser.

3.31 The following actors or functions are involved on the supply side, generally representing the service provider (this is a non-exhaustive list):

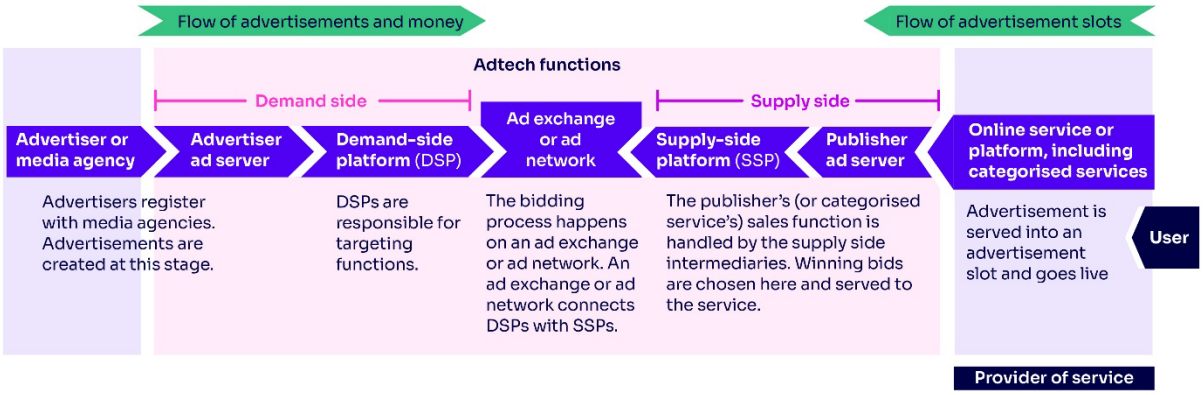
a) supply-side platforms (SSPs) that sell the advertising inventory on a service. An SSP connects to multiple DSPs and collects bids from them. If the provider is using a single SSP then that SSP decides the winning bid.
b) publisher ad server that manages the advertising inventory on a service and selects the winning bid from the SSPs that it is connected to. Generally, a provider will use a publisher ad server if the provider engages several SSPs to sell their inventory.

3.32 Other actors in the supply chain can include:

a) an agency trading desk which can manage advertising campaigns for advertisers;
b) an ad network which is involved in the selling of advertisements;
c) an ad exchange which acts as a marketplace for advertisements; or
d) a data management platform which collects and manages data.

[78] CMA, 2020. Appendix M: intermediation in open display advertising, p.3. [accessed 22 June 2026].

Figure 3.2: Simplified diagram of an open-display supply chain.[79]



Where relevant, we have used terms familiar to the advertising industry to describe the supply chain.
At the end of the supply chain, we use terminology consistent with the Online Safety regime.
'Provider', 'categorised service' and 'user' are terms consistent with the Online Safety Act.
The provider of the service may also provide other functions in the supply chain, not shown here.

3.33 The open-display supply chain consists of a wide range of actors, some of which will not be integrated with the service the provider is serving advertisements to users on.

3.34 This is a generalised summary of the process and there are significant variations based on how bids are submitted and how advertising intermediaries engage with each other. We also note that this supply chain is dynamic and constantly evolving.

Applying measures in open-display supply chains

3.35 Service providers may or may not play an active role across the open-display supply chain. This could be because some of the adtech functions may not be integrated with the service or because some of the functions may be performed by an intermediary that is a separate third party to the service. As described in paragraphs 3.31 to 3.33, decisions around the placement of advertisements on services that use the open-display market are shared among several intermediaries. This may limit the role that a provider plays over advertisement placement on its service(s). In some circumstances, this could make it difficult for service providers to take steps to protect users from fraudulent advertisements. For example:

- Because a publisher ad server or an SSP is responsible for choosing winning bids from the auction process, the provider of the categorised service on which the advertisement is being placed may not be able to see who the advertiser is and what advertisement is being placed on the service. This may make it more difficult to moderate advertisements.
- Because the advertiser might register with a media agency or a DSP – and not the service itself – the provider may not be able to directly place account checks on the advertiser because the advertiser is on the other end of the supply chain.

3.36 Despite this, providers have discretion over the process to place advertisements on their service(s). For example, providers have decision-making power over which advertising

[79] This simplified diagram draws from similar diagrams produced by SparkNinety (for the UK DCMS) and the CMA. The diagrams have been adapted to show key concepts relating to the Act and the Fraudulent Advertising duties. Source: SparkNinety, 2022. Online advertising programme market insights: final report, p.35. [accessed 22 June 2026]; CMA, 2020. Online platforms and digital advertising, p.265. [accessed 22 June 2026].

intermediaries (or ad networks) they work and have arrangements with. These arrangements often include parameters and blocklists, where providers set out what advertisers they do not want advertisements from, and what types of advertisements they do not want to see on a service.[80]

3.37 There are also a range of tools that can be deployed across the open-display supply chain. These tools are generally offered by third-party actors or standards bodies within the advertising industry, and can be used by providers as alternatives to in-house safety measures. These tools can perform various functions related to, for example, detecting and blocking harmful or non-compliant advertisements or advertisers. For example, cybersecurity firm Confiant offers security tools for advertisement security and quality, with a focus on detecting and blocking advertisements in real time.[81] Tools from the IAB's Tech Lab also offer similar safety measures: buyers.json, for example, allows sellers (in this case, providers of categorised services) to see who is buying their inventory, which can help sellers to better monitor advertisements being placed on services.[82] Generally, we understand that both providers and intermediaries can deploy these kinds of tools.

Direct deal advertising

3.38 Sometimes, part of the decision around which advertisement is placed on a service can be determined by any direct deals an advertiser has made with a service provider. Providers can enter into a direct agreement with an advertiser to place advertisements from their business on its service (or services). In these scenarios, the provider usually knows who the buyer is.

3.39 Direct deals can happen through the open-display market: supply-side platforms or ad servers can ensure that advertisements from advertisers with whom the service has a direct deal are given a preferential position in a bid. This can happen through programmatic guaranteed deals[83] – where advertisers and providers agree to a number of impressions – or through private marketplaces within private ad exchanges.[84]

3.40 Direct deals can also happen in a vertically integrated supply chain that is owned-and-operated.

[80] The IAB OpenRTB Standard is widely used across the advertising ecosystem, and includes provisions for 'blocklists' which allows providers to specify categories of advertisements that it does want served to users of its service(s).
[81] For more information, see Confiant, no date. https://www.confiant.com/solutions/quality. [accessed 26 June 2026].
[82] IAB, 2021. IAB TechLab: buyers.json specification – version 1.0, p.5 [accessed 22 June 2026].
[83] For example, see: Google Display and Video 360 Help, no date. Programmatic Guaranteed deals. [accessed 22 June 2026].
[84] Ofcom and Integrity Institute, 2026. Fraudulent advertising and account integrity: Expert insights on best practice.

4. Causes and impacts of fraudulent advertising

What is this section about?

Fraud is the most common crime in the UK, with an estimated 4.4 million incidents taking place in 2025. The Home Office estimated that in 2023 to 2024[85] the total economic and social cost of fraud against individuals was £9.2 billion. Advertising is the second most common way fraudsters reach victims online, and they are increasingly using paid-for advertisements to target users at scale.

The impact of fraudulent advertising can be severe. Victims not only lose money, but often suffer emotional distress, erosion of trust, and lasting effects on their lives. There are also wider societal and business impacts, as proceeds can fund organised crime and the loss of trust in advertisements undermines legitimate businesses. These impacts can damage communities, distort markets and disproportionately affect smaller firms.

Fraudulent advertising is a highly adversarial harm type, with perpetrators continuously adapting and evolving their tactics to evade detection. Perpetrators use any method they can to defraud users, meaning that fraudulent advertising manifests in diverse and complex ways and across a range of advertisement types – including fraudulent investment, retail, and medical advertisements.

Fraudsters exploit new technology such as artificial intelligence (AI), take advantage of social trends, and leverage the credibility of public figures and trusted brands to deceive users. They often operate through large-scale, coordinated networks and deploy tactics such as impersonation and account takeover to evade detection and increase the reach of their campaigns.

These diverse manifestations and adversarial methods give rise to a range of risky characteristics within both advertisement content and advertising accounts. While such characteristics may also appear in legitimate advertising, certain patterns can indicate that a paid-for advertisement is fraudulent. The characteristics we set out include the impersonation of public figures and brands, cloaked landing pages and unusual URLs, the use of generative AI and 'deepfakes', and suspicious account behaviours.

Anyone can be a victim of fraudulent advertising; evidence suggests that no one group is the most vulnerable, but rather that individuals may fall victim based on their circumstances, with some users being more likely to be targeted by or fall victim to specific types of fraudulent advertising.

Consultation questions

- Do you have any comments on Ofcom's assessment of the causes and impacts of fraudulent advertising? Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.
- Do you agree with the examples of risky characteristics we have provided? Please provide any arguments and supporting evidence.

[85] Note that this relates to the year ending March 2024.

Introduction

4.1 This section sets out our analysis relating to the causes and impacts of fraudulent advertising. We set out evidence that demonstrates that fraudulent advertising happens at large scale as perpetrators increasingly use paid-for advertising on online user-to-user and search services (which we refer to as 'online advertising') to reach users quickly and in large numbers, which leads to significant impacts on UK users.

4.2 We also highlight the dynamic and evolving nature of fraudulent advertising. This includes the diverse ways in which it manifests online across user-to-user and search services, as well as the tools and tactics used by perpetrators and the mechanisms used to defraud users. We provide examples of characteristics that are commonly observed in the content of fraudulent advertisements and the advertising accounts that post them. Ultimately, we acknowledge the evolving and adversarial nature of fraudulent advertising and that it is likely to continue to grow as technology, such as artificial intelligence (AI), becomes more sophisticated. It would therefore be extremely challenging to provide a comprehensive list of risky characteristics, and instead we recognise that this may vary across the diverse services in scope of these draft Fraudulent Advertising Codes of Practice and is likely to change over time.

4.3 We note that not all of the evidence in this section relates directly to fraudulent advertisements as defined in the Online Safety Act 2023 (the Act). We have also drawn on evidence that relates to fraud more widely, or that uses different definitions of fraudulent advertisements. We make clear where this is the case. We provisionally consider that using evidence that relates to fraud more widely or relies on a different definition of fraudulent advertisements is useful in this case, as it helps to build an understanding of the overall scale and impact of fraudulent advertising, where there is limited evidence relating specifically to fraudulent advertisements as defined by the Act. For clarity, we refer to wider fraud in this section as 'fraud', and fraudulent advertisements under the Act's definition as 'fraudulent advertisements'.

Fraudulent advertising and how it manifests online

What is fraudulent advertising?

4.4 It is not always clear to a user whether content they encounter online is a paid-for advertisement (as defined in the Act), and therefore whether it could be a fraudulent advertisement that is in scope of these draft Codes.[86] There are other ways that people or businesses can advertise online that do not involve paid-for advertising, for example, through promoting brands or products through influencer posts using user-generated content.

4.5 Because the distinguishing features that make content a paid-for advertisement relate to payment and contractual arrangements rather than outward appearance, they are not always visible to users. As a result, factors such as the way an advertisement looks, the account posting it, and any labels that point towards it being an advertisement may not

[86] See Volume 1, Section 2, 'Introduction' for an explanation of paid-for advertisements as well as fraudulent advertisements and service providers' duties relating to them.

reliably indicate whether content is a paid-for advertisement under the Act's definition, and so whether it could be a fraudulent advertisement in scope of these draft Codes.

4.6 Ofcom research supports this by highlighting the difficulties people can have in understanding what a paid-for advertisement is. In one study, although most respondents felt confident to identify specific paid-for advertisements that are relevant to the Act's definition, many misidentified examples of advertisements shown to them in practice.[87]

4.7 Businesses and others in the advertising industry may incorrectly associate fraudulent advertising with 'ad fraud'.[88] Ad fraud refers to the deceptive practice of inflating advertising metrics to generate financial gain, which is a significantly different concept to how fraudulent advertising is defined by the Act. While ad fraud relates to advertisers being defrauded, this section and our draft Fraudulent Advertising Codes concern individuals in the UK who are defrauded through paid-for advertisements.

4.8 There is widespread concern about fraudulent advertising across industry and the public. Research by the Advertising Standards Authority (ASA) suggested that 64% of UK online adults are concerned about scams or fraudulent advertising,[89] and many industry and civil society stakeholders have also expressed concern and the need for more to be done to tackle it.[90]

4.9 The ASA's research also shows that 84% of UK online adults are concerned about misleading advertisements, 44% are concerned about the use of deepfakes in advertising, and 32% are concerned about the use of AI in advertising.[91] Although these features do not necessarily make a paid-for advertisement fraudulent, this section will explain how these features can appear in fraudulent advertising.[92] There is also concern over the use of AI to

---

[87] In Ofcom research, following the introduction of specific types of online paid-for advertisements that are relevant to the Act's definition, 80% of respondents immediately felt confident (30% very confident and 50% fairly confident) in identifying them accordingly. However, only 3% answered correctly out of all six examples and more than half (52%) only got three or fewer answers correct. Source: Ofcom, 2026. Online paid-for advertisements research.

[88] Ofcom, 2026. Online advertising pathways: qualitative research report.

[89] Note that this refers to scams or fraudulent advertising more generally (not just paid-for fraudulent advertisements per the Act's definition). Respondents selected 'scams/fraudulent advertising' from a list of advertising-related issues across different media. The research was conducted by YouGov among a sample of 6,808 online adults aged 16+. Source: ASA, 2025. Understanding Advertising: Context and Concerns. [accessed 16 February 2026].

[90] ASA response to 2024 Call for Evidence: Third Phase of Online Safety Regulation, pp.2 and 3; Carnegie UK, 2021. Coalition Of Consumer Groups, Charities And Industry Bodies Calls For Inclusion Of Paid For Online Advertising In Online Safety Bill. [accessed 18 March 2026]; Juniper Research and Revolut, 2026. Protecting Users from Scam Ads: A Call for Social Media Platform Accountability. [accessed 13 February 2026]; Middle Tech Coalition (formerly Mid Size Platform Group) response to 2024 Call for Evidence, p.5; Money Saving Expert (MSE), 2021. Martin Lewis, Sir Richard Branson, Deborah Meaden and other public figures issue plea to the PM to put scam ads in the Online Safety Bill. [accessed 18 March 2026]; Revolut response to 2024 Call for Evidence, pp.1 and 2; [✂] response to 2024 Call for Evidence, [✂]; UK Finance response to 2024 Call for Evidence, p.2; Which? response to 2024 Call for Evidence, p.1.

[91] The ASA defined misleading advertisements as "any advertising that you would consider, on the basis of what you know or very strongly suspect to be, deceptive or to give the wrong idea or impression of a product or service. This can be either intentional or unintentional and by omission." Respondents selected use of deepfakes and use of AI from a list of advertising-related issues across different media. Source: ASA, 2025. Understanding Advertising: Context and Concerns. [accessed 16 February 2026].

[92] Even if an advertisement is not fraudulent, it may be unlawful for other reasons, for example under consumer law.

spread disinformation through AI news aggregators and AI-generated advertisements.[93] We note only paid-for advertisements that are displayed on Category 1 and 2A services and amount to a fraud and financial services offence as specified in section 40 of the Act are in scope of the fraudulent advertising duties under the Act.

4.10 We highlighted in our Illegal Harms Register of Risks (Illegal Harms Register) that fraud offences can manifest in complex ways.[94] This also applies to fraudulent advertising, where perpetrators use a variety of methods to defraud users which can result in varied and complex manifestations of fraud through online advertising. We explain this further and provide examples of the forms fraudulent advertisements can take in the sub-sections 'How fraud manifests through online advertising' and 'Risky characteristics'.

Scale of fraudulent advertising

4.11 Fraud is the most common crime in the UK,[95] with an estimated 4.4 million incidents taking place in England and Wales in the year ending December 2025.[96] Ofcom research has shown that almost a third (29%) of UK adults online report they have seen or experienced scams, fraud or phishing in the previous four weeks.[97] The resulting impact is substantial: the Home Office estimated that the total economic and social cost of fraud against individuals in England and Wales in the financial year ending March 2024 was £9.2 billion.[98]

4.12 Ofcom research found advertising is the second most common content type used by scammers to reach their victims online, with 20% of scam or fraud victims reporting being contacted via adverts.[99] Further evidence indicates that online advertisements account for 11% of total scam and fraud experiences,[100] and that the volume of fraudulent advertisements is likely to be increasing.[101] Around half of UK adult users say they have

---

[93] Centre for Emerging Technology and Security, 2026. Adding Fuel to the Fire: AI Information Threats and Crisis Events. [accessed 16 March 2026].

[94] Our December 2024 Statement on Protecting People from Illegal Harms Online (December 2024 Statement), Illegal Harms Register, pp.237 to 239.

[95] National Economic Crime Centre, 2025. National Economic Crime Centre Annual Report. [accessed 25 March 2026]; UK Finance, 2025. Annual Fraud Report 2025. [accessed 5 February 2026].

[96] The Crime Survey is conducted in England and Wales among those aged 16+. Office for National Statistics (ONS), 2026. Crime in England and Wales: Year ending December 2025. [accessed 4 March 2026]. The Scottish Crime and Justice Survey, based on those 16+, found there was an estimated 494,000 fraud incidents in Scotland in 2024/25. Scottish Centre for Social Research, 2026. Scottish Crime and Justice Survey 2024/25: Main findings. [accessed 26 June 2026]. The equivalent survey in Northern Ireland does not give specific breakdowns for fraud, however evidence suggests that fraud in Northern Ireland is a similarly common crime. Police Service of Northern Ireland, 2025. Police Recorded Crime in Northern Ireland 1998–99 to 2024–25. [accessed 26 June 2026].

[97] Online adults aged 18+. Ofcom, 2026. Online Experiences Tracker, Wave 9.

[98] Home Office, 2026. Economic and social cost of fraud 2023 to 2024. [accessed 21 April 2026]; See also the sub-section 'Impact of fraudulent advertising' for further detail on impacts.

[99] Note this relates to advertisements respondents "saw on websites/apps, social media sites or video-sharing platforms", so does not specifically relate to paid-for advertising as defined by the Act. Research was conducted with 2,097 UK online adults aged 18+. Source: Ofcom, 2023. Executive Summary Report: Online Scams & Fraud Research.

[100] Online advertisements were defined in this study as advertisements on non-social media websites or on social media websites, blogs or forums. This figure comes from an EU-wide survey (which also included the UK, Iceland and Norway) carried out by the European Commission among residents aged 18+. Source: European Commission, 2020. Survey on "Scams and Fraud experienced by consumers". [accessed 24 March 2026].

[101] Sparkninety, 2022. Online Advertising Programme Market Insights. [accessed 13 March 2026]; Center for Countering Digital Hate, 2026. Scambook: How Meta helps Medicare scammers target seniors. [accessed 15

seen potentially fraudulent online paid-for advertisements, with over a third saying they see them frequently.[102]

4.13 Most available data does not specify the origin of fraud cases and whether they relate to paid-for advertising. However, as we set out in Annex 8, 'Further detail on economic assumptions and analysis', we estimate that between 181,000 and 202,000 UK users lose money because of engaging with a fraudulent advertisement every year.[103] We also set out there that we have taken a cautious approach not to overstate these figures. This is consistent with evidence we outline in paragraph 4.14 which suggests that fraud goes largely under-reported, and so the number of cases may be much higher.

4.14 Estimates indicate that fewer than one in seven fraud offences are reported to the police or Action Fraud.[104] For fraudulent advertisements specifically, Ofcom research found that just over two in five UK online adults who interacted with a potentially fraudulent paid-for advertisement reported it.[105]

4.15 The nature of fraudulent advertising means that it is perpetrated through methods designed to deceive those who encounter the advertisement into thinking they are interacting with a legitimate advertisement. The nature of the relevant offences is such that they will often go undetected and therefore be under-reported. The British and Irish Law Education and Technology Association (BILETA) noted that the individuals who do report fraudulent advertisements tend to be those with consumer awareness or the relevant knowledge of the harm and how it operates, rather than those who are likely to fall victim to the fraud itself.[106]

4.16 Ofcom research suggests that some users are not always able to accurately identify fraud in online advertising. For example, when shown an inauthentic paid-for advertisement on a user-to-user service featuring a public figure who repeatedly said that they do not do advertisements, 23% of respondents still incorrectly identified it as genuine, while 18% said they were unsure. This was also observed on search services, where 38% of respondents incorrectly identified a fraudulent advertisement as genuine, with 24% unsure.[107] Further Ofcom research indicates that many internet users struggle to identify paid-for advertisements on search services.[108] This means that without knowing that they are interacting with a fraudulent advertisement – or even that a search result they encountered

---

May 2026]; Juniper Research and Revolut, 2026. Protecting Users from Scam Ads. [accessed 13 February 2026].

[102] Of those who have ever encountered or seen potentially fraudulent online paid-for advertisements (51%), 13% said they see it very frequently (almost every time when online), 23% said frequently (more than half the time) and 35% said sometimes (about half the time). Ofcom, 2026. Online paid-for advertisements research.

[103] This estimate is based on analysis that combines different evidence sources. See Annex 8, 'Further detail on economic assumptions for more detail.

[104] This refers to fraud offences generally rather than specifically in relation to fraudulent advertising. Source: ONS, 2023. Crime in England and Wales: year ending June 2023. [accessed 5 February 2026].

[105] When users realised they had experienced a scam because of an online paid-for advertisement, 43% reported it as one of the action(s) they took. For example, 20% reported it to the online platform and/or their bank or finance provider, 8% reported it to Report Fraud (formerly known as Action Fraud) and 2% reported it to Citizens' Advice. Ofcom, 2026. Online paid-for advertisements research.

[106] BILETA response to 2024 Call for Evidence, p.35.

[107] Ofcom, 2026. Online paid-for advertisements research.

[108] 37% of search engine users aged 16+ said they were confident in identifying online advertising but did not identify sponsored links when tested. Ofcom, 2026. Adults' Media Use and Attitudes report.

was a paid-for advertising placement – users may struggle to identify where fraudulent activity originated.

4.17 The Integrity Institute's insight report also highlights that some forms of fraud will not be captured by user reporting. For example, if a user receives a counterfeit product, they may not know until days or weeks later and may not be able to track down the advertisement that led them to the product.[109] Ofcom research showed that it took 21% of users from a few days to more than a month to realise that an online paid-for advertisement they engaged with was fraudulent.[110] By this point, it is likely to be difficult to track down and report the fraudulent advertisement. This combined evidence shows that under-reporting can happen because people can fail to identify fraudulent advertisements or become aware that they have interacted with one too late to report it. Another factor may be that victims sometimes can suffer losses so small that they are not aware they are a victim.[111]

4.18 Under-reporting can also occur because of a lack of awareness around how to report a fraudulent advertisement. The process may require multiple steps or actions, which can also dissuade users from reporting.[112] Furthermore, Ofcom research found that the perceived ineffectiveness of reporting can be a significant barrier.[113] For some individuals, the emotional impacts of fraud can act as a barrier to reporting the crime, which we discuss further in the sub-section 'Impact on individuals'.

How fraud manifests through online advertising

4.19 Many online services display paid-for advertisements, and a single advertisement can be seen by millions of users.[114] Due to this, online advertisements are used by perpetrators to reach consumers at a substantial scale,[115] and have frequently allowed criminals to defraud others.[116]

4.20 Evidence shows that fraudulent advertising is highly adversarial.[117] Perpetrators are highly motivated, using whatever methods they can to commit fraud and looking to exploit any opportunities offered by new technology and social trends.[118] Fraud and its perpetrators' behaviours are dynamic and adaptable,[119] and in a context with rapidly developing

---

[109] Ofcom and Integrity Institute, 2026. Fraudulent advertising and account integrity.
[110] Ofcom, 2026. Online paid-for advertisements research.
[111] Victims' Commissioner, 2021. Who suffers fraud? Understanding the fraud victim landscape. [accessed 10 February 2026].
[112] BILETA response to 2024 Call for Evidence, p.35; Ofcom, 2026. Behavioural Audit of Services with Advertisement Functionality.
[113] Forty-five per cent of UK users who did not report a potentially fraudulent advertisement said it was because of the perceived ineffectiveness of reporting. Source: Ofcom, 2026. Online paid-for advertisements research.
[114] UK Finance response to 2024 Call for Evidence, pp.4 and 5.
[115] Juniper Research and Revolut, 2026. Protecting Users from Scam Ads. [accessed 13 February 2026]; National Crime Agency, 2026. Online Harms. [accessed 17 March 2026]; Revolut response to 2024 Call for Evidence, p.4; Which? response to 2024 Call for Evidence, p.2.
[116] Gen Digital, 2026. The Scam Ad Machine. [accessed 3 March 2026].
[117] Google (confidential) response to 2024 Call for Evidence, p.54; Ofcom and Integrity Institute, 2026. Fraudulent advertising and account integrity; [✂] response to 2024 Call for Evidence [✂].
[118] Google (confidential) response to 2024 Call for Evidence, p.54; Ofcom and Integrity Institute, 2026. Fraudulent advertising and account integrity; Which? response to 2024 Call for Evidence, p.2.
[119] BILETA response to 2024 Call for Evidence, p.35; Google (confidential) response to 2024 Call for Evidence, pp.54 and 55; Ofcom and Integrity Institute, 2026. Fraudulent advertising and account integrity; [✂] response to 2024 Call for Evidence [✂]; MSE response to 2024 Call for Evidence, p.28; UK Finance, 2025. Annual Fraud

technologies and the range of diverse services that may be in scope of these draft Codes, the nature of the harm and its manifestations are likely to continue to evolve.

4.21 Fraudulent advertisements often use deceptive features designed to mimic legitimacy and persuade users to engage. A prominent example is impersonation, including the use of the likeness of well-known figures and celebrities to lend credibility to fraudsters' claims or to entice users to click on the advertisement.[120] Other such features include the use of persuasive language and attention-grabbing content. In practice, many of the features employed by fraudsters overlap and are used in combination; for example, AI-generated content may be used to create more convincing impersonation or to enhance other deceptive elements. We discuss the use of these features and how they can be a sign that a paid-for advertisement is fraudulent in further detail in the sub-sections 'Tools and techniques used in fraudulent advertising' and 'Risky characteristics'.

4.22 In the following sub-section, we explain the types of fraudulent advertisements that commonly appear online and how bad actors use online advertising to carry out fraud.

Types of fraudulent advertisements

4.23 Perpetrators can carry out fraud through a variety of types of paid-for advertisements. Some common examples include:

- **Fraudulent investment advertisements:** These advertisements feature fraudulent investment products or platforms, and evidence suggests they are becoming increasingly popular among perpetrators.[121] UK Finance data shows investment scams account for 38% of total losses from authorised push payment scams,[122] [123] and further evidence shows that 96% of these originate online.[124] Investment scams are also typically the highest value scams.[125] According to the Perimeter Report from the Financial Conduct Authority (FCA), some of the most serious harm from investment scams continues to come from businesses operating without FCA authorisation,[126] so there is an overlap between investment fraud targeting UK users and financial services advertising from unauthorised individuals and firms.
- **Fraudulent cryptocurrency advertisements:** Like fraudulent investment advertisements, these are a common type of fraudulent advertisement featuring fraudulent cryptocurrency

---

Report 2025. [accessed 5 February 2026]; Which? response to 2024 Call for Evidence, p.3; X response to 2024 Call for Evidence, p.4.

[120] Sparkninety, 2022. Online Advertising Programme Market Insights. [accessed 13 March 2026].

[121] Juniper Research and Revolut, 2026. Protecting Users from Scam Ads. [accessed 13 February 2026]; National Crime Agency, 2026. Online Harms. [accessed 17 March 2026].

[122] UK Finance defines an authorised push payment scam as "where customers are tricked into authorising a payment to another account controlled by a criminal." Source: UK Finance, no date. Over two thirds of all APP scams start online – new UK Finance analysis. [accessed 22 April 2026].

[123] Note that this figure relates to the first half of 2025. Source: UK Finance, 2025. Half Year Fraud Report 2025. [accessed 22 April 2026].

[124] UK Finance analysed authorised push payments scams by origin channel, classifying email, social media, websites (incl. auction sites), and apps (incl. dating) as online; non-online scams were initiated in person, by phone, or by text. UK Finance, no date. Over two thirds of all APP scams start online – new UK Finance analysis. [accessed 22 April 2026].

[125] Innovate Finance response to 2024 Call for Evidence, pp.7 and 8; Revolut (confidential) response to 2024 Call for Evidence, p.6.

[126] FCA Perimeter Report 2024, referenced in FT Adviser, 2024. FCA: We do not always have the power to act. [accessed 15 May 2026].

products or platforms.[127] The scams carried out through these advertisements are also likely to involve larger sums of money according to the ASA.[128]

- **Fraudulent retail advertisements:** These advertise products for sale, often at highly discounted 'too good to be true' prices or featuring dramatic closing down sales.[129] These advertisements can also include false claims about the company and the products being sold and can include the use of AI.[130]
- **Fraudulent medical advertisements:** These advertise products such as weight loss products[131] and CBD gummies,[132] and can promise exaggerated or 'miracle' results.[133]
- **Fraudulent travel advertisements:** These often advertise cheap or highly discounted flights and local travel.[134]
- **Fraudulent employment advertisements:** These advertise fake job listings.[135]
- **Fraudulent insurance advertisements:** These advertise fraudulent insurance products and can involve 'paid ad spoofing', whereby fraudsters use paid-for search advertisements to appear at the top of search results when users search for their insurer to make a claim.[136]

Tools and techniques used in fraudulent advertising

4.24 Evidence indicates that bad actors use a range of tools and techniques to carry out fraud through online advertising, which we explain in the rest of this sub-section.

4.25 Stakeholders told us that perpetrators of fraudulent advertising take advantage of emerging technologies to avoid detection and deceive users.[137] This includes generative AI (GenAI), which can be used, for example, to produce text or create deepfake images or videos. Ofcom research found that bad actors are incentivised to use GenAI because it is simple and cheap to use, and it can rapidly produce highly convincing content from scratch at low cost. For example, according to one safety technology firm, the cost to clone a voice fell from upwards of $10,000 to just a few dollars in the space of a year.[138] This has led to widespread prevalence of this technology in fraudulent advertising. Ofcom research shows

---

[127] ASA response to 2024 Call for Evidence, p.4; Cifas response to 2024 Call for Evidence, p.1; Financial Conduct Authority (FCA), 2026. Crypto investment scams. [accessed 20 March 2026].
[128] ASA response to 2024 Call for Evidence, p.4.
[129] Sparkninety, 2022. Online Advertising Programme Market Insights. [accessed 13 March 2026]; ASA, 2025. A year in scams: 2024 update on Scam Ad Alert System. [accessed 3 February 2026]; ASA, 2026. A year in scams: 2025 update on Scam Ad Alert System. [accessed 9 February 2026].
[130] Which, 2025. Shopping scams: know how to spot a rogue retailer. [accessed 7 May 2026].
[131] ASA response to 2024 Call for Evidence, p.4; Sparkninety, 2022. Online Advertising Programme Market Insights. [accessed 13 March 2026]; Which?, 2025. Watch out for the Nixol diet pill scam. [accessed 5 February 2026], Which?, 2026. Deepfake doctors used to peddle weight-loss patches. [accessed 15 June 2026].
[132] ASA response to 2024 Call for Evidence, p.4; Sparkninety, 2022. Online Advertising Programme Market Insights. [accessed 13 March 2026].
[133] Sparkninety, 2022. Online Advertising Programme Market Insights. [accessed 13 March 2026]; Ofcom, 2023. Executive Summary Report: Online Scams & Fraud Research.
[134] ASA, 2025. A year in scams: 2024 update. [accessed 3 February 2026]; Middle Tech Coalition (formerly Mid Size Platform Group) response to 2024 Call for Evidence, p.5.
[135] Cifas response to 2024 Call for Evidence, p.2; Google, 2025. Our latest fraud and scams advisory. [accessed 5 February 2026].
[136] We discuss this in further detail in the sub-section 'Risky characteristics'; See also the Association of British Insurers (ABI) response to 2024 Call for Evidence, p.26.
[137] ABI response to 2024 Call for Evidence, p.27; BILETA response to 2024 Call for Evidence, p.35; Google (confidential) response to 2024 Call for Evidence, p.54; MSE response to 2024 Call for Evidence, p.28; X response to 2024 Call for Evidence, p.4.
[138] Ofcom, 2024. Deepfake Defences: Mitigating the Harms of Deceptive Deepfakes. [accessed 6 March 2026].

that 43% of UK online adults (16+) said they had encountered a deepfake in the previous six months, with 45% of those being in a fraudulent or scam advertisement.[139] Evidence suggests that bad actors also use GenAI to manipulate audio and visual content to fabricate identity documents in order to bypass security measures including onboarding processes implemented by financial institutions,[140] a technique which also has the potential to be used to carry out fraud through online advertising. Because it is easy to access and operate these technologies, their use in fraudulent advertising appears to be becoming increasingly common,[141] and it will likely continue to increase in volume and sophistication in the coming years.[142] We expect that this will drive increases in the overall volume of fraudulent advertising that people are exposed to.

4.26 We also heard from stakeholders that bad actors often take advantage of social trends and focus on advertising that will connect with consumers.[143] This can include using sensationalist stories about celebrities to grab attention,[144] incorporating external events and news such as policy changes,[145] and exploiting events like Black Friday when users are likely to be engaging in higher amounts of shopping than usual.[146]

4.27 In connecting with users, a common tactic employed by fraudsters is impersonating legitimate brands, organisations or well-known figures.[147] In online fraud more widely, Ofcom research found that impersonation fraud was the most commonly experienced fraud type, reported by 51% of respondents.[148] This technique is also used in fraudulent advertising, where fraudsters might impersonate these entities through the content they use (for example, a name, image or logo) or through the account sharing the advertisement. Research shows that users often engage with these advertisements, with 43% of UK users who interacted with a potentially fraudulent advertisement saying it featured a well-known brand or public body, and 24% saying it featured a well-known individual.[149] Fraudsters exploit the credibility that well-known figures or brands offer advertisements and users' trust in them to increase the likelihood of engagement with fraudulent advertisements. Evidence indicates that there is a growing trend of

---

[139] Ofcom, 2024. Online Safety open data, Online safety open data, Deepfakes (older teenagers and adults).
[140] KPMG, no date. CDD and Generative AI – Risks of KYC Fraud. [accessed 29 April 2026].
[141] AGENCY response to 2024 Call for Evidence, pp.14 and 15; ASA, 2026. A year in scams: 2025 update. [accessed 9 February 2026]; BILETA response to 2024 Call for Evidence, p.51; Cifas response to 2024 Call for Evidence, p.5; MSE response to 2024 Call for Evidence, p.37.
[142] ABI response to 2024 Call for Evidence, p.34; Cifas response to 2024 Call for Evidence, p.5; PWC and Stop Scams UK, 2023. Impact of Artificial Intelligence on Fraud and Scams. [accessed 6 March 2026].
[143] Google (confidential) response to 2024 Call for Evidence, p.54; Which? response to 2024 Call for Evidence, p.2.
[144] Which? response to 2024 Call for Evidence, p.2.
[145] For example, policy changes on winter fuel payments prompted advertisements linking to fake government websites that sought users' personal and financial data. Source: Which?, 2024. Beware of bogus 'Winter Fuel Payments' ads on Facebook and Instagram. [accessed 12 March 2026].
[146] BILETA response to 2024 Call for Evidence, pp.33 and 34.
[147] ASA response to 2024 Call for Evidence, p.4; ASA, 2026. A year in scams: 2025 update. [accessed 9 February 2026]; Ofcom and Integrity Institute, 2026. Fraudulent advertising and account integrity; Revolut response to 2024 Call for Evidence, p.3.
[148] The research defined impersonation fraud as follows: "Fraudsters pretend to be from a legitimate organisation (e.g. a financial institution, the NHS, lottery institution, solicitors, government officials) and request a payment or information from you." Impersonation fraud was the most commonly experienced fraud type from a list of 11 tested. Source: Ofcom, 2023. Executive Summary Report: Online Scams & Fraud Research.
[149] Ofcom, 2026. Online paid-for advertisements research.

impersonation in fraudulent advertising, driven in part by the increasing use of AI to create more convincing and scalable content.[150] We discuss impersonation further in the sub-section 'Risky characteristics'.

4.28 Evidence indicates that the distribution of fraudulent advertisements can be coordinated by criminal operations that deploy extensive networks of accounts.[151] Criminals can use these networks to disseminate large volumes of fraudulent advertisements across services. A study by Gen Digital found that more than half (56%) of 'scam ads' on Meta services came from the same 10 advertiser entities – they say they "repeatedly traced clusters of campaigns back to payers and infrastructure linked to China and Hong Kong, operating fleets of short-lived pages created almost exclusively to run ads."[152] A notable example is Quantum AI, widely described as an unauthorised and fraudulent investment scheme that operated across numerous cloned websites, social media platforms, and jurisdictions. It relied heavily on deceptive marketing, including deepfake celebrity and political endorsements, fabricated news articles, and synthetic testimonials to lure victims. Governments and regulators issued multiple warnings after identifying AI-generated advertisements impersonating public figures, and the scam is characterised in public reporting as part of a coordinated international fraud network.[153]

4.29 To evade detection and make it harder to trace the fraud back to the perpetrator, bad actors often use fake accounts[154] or take over accounts that were previously legitimate.[155] Evidence indicates that fraudsters can automatically generate large numbers of fake accounts, using automated scripts to populate profiles with usernames, photos and contact information.[156] Account takeovers can be attractive for fraudsters as they can allow them to bypass onboarding and verification checks,[157] and also because research indicates that users are more likely to trust established brands.[158] Evidence indicates that advertising accounts acquired by bad actors are also being sold illicitly. This can allow fraudsters to

---

[150] ASA, 2026. A year in scams: 2025 update. [accessed 9 February 2026]; BILETA response to 2024 Call for Evidence, p.51; Google, 2024. Ads Safety Report. [accessed 10 March 2026].

[151] Note that these evidence sources do not specify whether they are referring to fraudulent advertisements per the Act's definition. Sources: Which?, 2022. A scammer can make nearly £1 million a day through fraudulent online adverts. [accessed 6 March 2026]; The Bureau of Investigative Journalism, 2024. Doctored Footage and Hijacked Accounts: Anatomy of a Deepfake Scam. [accessed 6 February 2026]; Reset Tech, 2025. The Dormant Danger: How Meta Ignores Large-Scale Inauthentic Behavior Networks of Malicious Advertisers. [accessed 6 February 2026]; Gen Digital, 2026. The Scam Ad Machine. [accessed 3 March 2026].

[152] This study was carried out over a 23-day period, in which Gen Threat Labs analysed 14.5 million advertisements running on Meta platforms across the EU and UK. The 'scam ads' they identified were those that pointed to "infrastructure associated with e-commerce scams, phishing campaigns, malware distribution and other consumer-facing threats." Source: Gen Digital, 2026. The Scam Ad Machine. [accessed 3 March 2026].

[153] The Bureau of Investigative Journalism, 2024. Doctored Footage and Hijacked Accounts. [accessed 6 February 2026]; Which?, 2024. We exposed a global AI scam. [accessed 6 March 2026].

[154] AGENCY response to 2024 Call for Evidence, p.10; Reset Tech, 2025. The Dormant Danger. [accessed 6 February 2026]; X response to 2024 Call for Evidence, p.4.

[155] ASA (confidential) response to 2024 Call for Evidence, pp.6 and 7; Check First, 2024. Facebook Hustles: The Hidden Mechanics of a Scam Machinery Impersonating News Organisations and Creators. [accessed 6 February 2026]; The Cyber Helpline response to 2024 Call for Evidence, p.26; Gen Digital, 2025. Gen Q1/2025 threat report. [accessed 9 March 2026]; Revolut (confidential) response to 2024 Call for Evidence, p.6; UK Finance response to 2024 Call for Evidence, p.18.

[156] Reset Tech, 2025. The Dormant Danger. [accessed 6 February 2026].

[157] UK Finance response to 2024 Call for Evidence, p.20; Which? response to 2024 Call for Evidence, p.11.

[158] Ofcom, 2026. Online paid-for advertisements research.

carry out fraudulent advertising campaigns, sometimes using the payment information of the real advertising account holders, with less risk of being identified due to the previous legitimacy of the accounts.[159] Evidence also suggests that account takeovers across various sectors, including social media, are increasing and may become even more common as AI technologies become more sophisticated.[160] Where fraudsters have been identified and banned from a service, they can use techniques such as creating new accounts (also known as 'phoenixing') or moving to secondary accounts (also known as 'lifeboating') to get around the ban.[161]

4.30 Research also highlights the use of affiliate marketing networks as a tool to enable fraud through online advertisements.[162] Affiliate marketing is the process whereby merchants, in this case bad actors, pay third-party affiliates to promote products or services through advertising. By using affiliates, fraudsters are able to expand their reach across multiple services, enabling them to access users at volume and increase the effectiveness of their fraudulent advertising campaigns.

Mechanisms to defraud users

4.31 Following users' engagement with a fraudulent advertisement, fraudsters employ various mechanisms designed to obtain money, data or access, which we describe in the rest of this sub-section. We also set out information about how interacting with a fraudulent advertisement can expose users to a range of secondary harms.

4.32 After interacting with a fraudulent advertisement, users may be led to a landing page that appears to be related to the advertisement, for example, offering the investment service or seeming to belong to the brand featured in the advertisement. From there, users may be prompted to enter their personal details or payment information as part of a phishing attempt.[163] Once bad actors obtain these personal details, they may contact individuals and defraud them outside of the service or website,[164] and a single scam may cross both online and offline channels and use multiple methods of communication.[165] Research found that 24% of users who had interacted with a potentially fraudulent advertisement reported being contacted by a scammer afterwards, with email being the most common method followed by phone and then text or social media.[166]

---

[159] DomainTools, 2025. Account Trafficking Websites in December 2024. [accessed 29 April 2026]; Tech Transparency Project, 2022. Facebook Black Market for Ad Accounts Raises New Scam, Election Interference Fears. [accessed 29 April 2026].

[160] Cifas, 2025. This is Fraudscape 2025. [accessed 9 February 2026]; Cifas, 2026. This is Fraudscape 2026. [accessed 16 March 2026]; Shaw, V. 2025. Major warning issued after surge in social media and email account hacks – how to protect yourself, Independent, 17 March. [accessed 19 June 2026].

[161] Note that this does not refer specifically to advertising accounts. Source: FCA response to June 2025 Additional Safety Measures Consultation, pp.4 and 6.

[162] Sparkninety, 2022. Online Advertising Programme Market Insights. [accessed 13 March 2026]; Quirium, 2025. The Hunt – From potential victim to 'depositor' in 20 min. [accessed 6 February 2026].

[163] AGENCY response to 2024 Call for Evidence, p.9; ASA response to 2024 Call for Evidence, p.4; ASA, 2025. A year in scams: 2024 update. [accessed 3 February 2026]; Middle Tech Coalition (formerly Mid Size Platform Group) response to 2024 Call for Evidence, p.5; MSE response to 2024 Call for Evidence, p.24.

[164] Which?, 2026. Social media deepfakes promote sham Quantum AI investment scheme. [accessed 18 March 2026].

[165] Google (confidential) response to 2024 Call for Evidence, p.55; Which?, 2023. Sharing data to tackle fraud. [accessed 18 March 2026].

[166] Email (42%) was most common channel used by scammers, followed by phone (33%), SMS/text or social media (both at 26%), then instant messenger (23%). Ofcom, 2026. Online paid-for advertisements research.

4.33 On search services, bad actors may use paid-for advertising to position fraudulent websites prominently in results when users search for a particular website or service, which can then enable fraud such as phishing. Fraudsters may impersonate legitimate services to steal login credentials which can then be used to take over genuine accounts. For example, evidence indicates that this method has been used to compromise advertising accounts on advertising platforms.[167] This demonstrates how the tactics and mechanisms used by bad actors can overlap within a single scam.

4.34 Fraudulent advertisements that may otherwise appear legitimate can also compromise a user's device or account, or lead to a website that will attempt to compromise a user's device or account.[168] This is also known as malvertising: "the use of malicious code in online ads to spread malware or steal information."[169] An Ofcom study showed that, of the UK users who said they had clicked on a potentially fraudulent advertisement, 12% noticed an unexpected file being downloaded on their device.[170] Evidence indicates that malvertising is becoming harder to spot, and Gen Digital cite this as a top threat to cybersecurity.[171]

Risky characteristics

4.35 Fraudulent advertising can take many forms, and the types, tactics and pathways described in the sub-section 'How fraud manifests through online advertising' can often overlap and shift as fraudsters adapt. These patterns give rise to a series of risky characteristics that can help identify potential fraud in online advertising or accounts that may post fraudulent advertisements. We outline common examples of these risky characteristics in the rest of this sub-section: taken alone or in combination, these characteristics can indicate an advertisement being fraudulent or an account sharing fraudulent advertisements. However, some of the same characteristics may also be seen in legitimate advertisements or accounts, so it is important to consider the context they appear in on services. Given the adversarial and changing nature of fraud and the different ways it might manifest through paid-for advertisements across services, our list of risky characteristics is not comprehensive, nor are the characteristics definitive evidence of fraudulent advertising.

Content risky characteristics

Impersonation through content

4.36 **Celebrities and public figures:** Fraudsters can use the likeness of well-known individuals (such as celebrities or public figures) to promote a product or service, or create fake news stories about the figure to grab users' attention.[172] Fraudsters may also use deepfakes of

[167] PC Mag, 2025. Hackers target Google Ad accounts – with Google Ad phishing schemes. [accessed 6 February 2026].
[168] Ofcom and Integrity Institute, 2026. Fraudulent advertising and account integrity; Peledie, R. 2024. How does malvertising work? [accessed 29 April 2024].
[169] We note that other bodies may define malvertising more broadly. Here we use the term to mean the definition provided. Source: Norton, 2026. Malvertising: What it is and how to prevent it. [accessed 9 March 2026].
[170] Ofcom, 2026. Online paid-for advertisements research.
[171] Gen Digital, 2026. Gen Q4 Threat Report Shows Scams Thriving Inside Ads, Feeds, and Video. [accessed 11 March 2026].
[172] AGENCY response to 2024 Call for Evidence, p.8; ASA response to 2024 Call for Evidence, p.4; ASA, 2025. A year in scams: 2024 update. [accessed 3 February 2026]; ASA, 2026. A year in scams: 2025 update. [accessed 9 February 2026]; BILETA response to 2024 Call for Evidence, p.33; MSE response to 2024 Call for Evidence, pp.24 and 25; [✂] response to our formal information request issued 26 June 2025; [✂] response to our

celebrities, and evidence tells us their use is increasing.[173] Data shows that users are more likely than average to lose money to fraudulent advertisements that feature a well-known influencer or social media personality (35% compared to 26%),[174] which may be attributed to the trust they have in these figures. Commonly used individuals include Martin Lewis, Elon Musk, Taylor Swift, Martin Wolf and Keir Starmer.[175]

4.37 **Brands:** Fraudulent advertisements can also impersonate well-known brands, with their name or logo being used to deceive users into thinking they are seeing a legitimate advertisement from the brand.[176] This includes retail brands, with evidence showing that fraudulent advertisements often falsely promote large discounts or sales across well-known brands,[177] as well as news publishers,[178] public bodies and banks.[179] On search services, evidence shows that perpetrators impersonate businesses such as telecom companies, insurance providers, retail brands and parking services so that their fraudulent sites appear at the top of users' search queries to then defraud them.[180]

Unusual URLs

4.38 The URL of a paid-for search advertisement, or of the landing page of a paid-for user-to-user advertisement (which users should be able to see within the advertisement), may look

---

formal information request issued 26 June 2025; [✂] response to our formal information request issued 26 June 2025; [✂] response to our formal information request issued 26 June 2025; [✂] response to our formal information request issued 24 November 2025; Stop! Think Fraud, no date. How to spot a fake online advert. [accessed 9 February 2026]; UK Finance response to 2024 Call for Evidence, p.13.

[173] AGENCY response to 2024 Call for Evidence, pp.14 and 15; ASA, 2025. A year in scams: 2024 update. [accessed 3 February 2026]; ASA, 2026. A year in scams: 2025 update. [accessed 9 February 2026]; BILETA response to 2024 Call for Evidence, p.51; Cifas response to 2024 Call for Evidence, p.5; GASA, 2024. Scammers Steal £11.4 Billion from Britons in 1 Year as 71% Fail to Report Scams – State of Scams in the United Kingdom 2024. [accessed 9 February 2026]; MSE response to 2024 Call for Evidence, p.37.

[174] Ofcom, 2026. Online paid-for advertisements research.

[175] ASA, 2026. A year in scams: 2025 update. [accessed 9 February 2026]; MSE response to 2024 Call for Evidence, p.37; MSE, 2025. Warning: The top 20 celebs used by scammers – beware ads featuring Martin Lewis, Taylor Swift, Elon Musk and more. [accessed 18 March 2026]; Which? response to 2024 Call for Evidence, p.12; Wolf, M. 2025. Playing 'whack-a-mole' with Meta over my fraudulent avatars, Financial Times, 25 April. [accessed 12 April 2026].

[176] ASA response to 2024 Call for Evidence, p.4; ASA, 2025. A year in scams: 2024 update. [accessed 3 February 2026]; [✂] response to our formal information request issued 26 June 2025; [✂] response to our formal information request issued 26 June 2025; [✂] response to our formal information request issued 24 November 2025; UK Finance response to 2024 Call for Evidence, p.20; Which? response to 2024 Call for Evidence, p.3; Which?, 2024. Social media platforms and search engines still littered with scam ads, Which? finds. [accessed 9 February 2026].

[177] Which?, 2024. Social media platforms and search engines still littered with scam ads. [accessed 9 February 2026]; Which?, 2025. Scam alert: Fraudsters impersonate Lidl in a series of fake ads. [accessed 9 February 2026].

[178] BBC response to 2024 Call for Evidence, p.5; Which?, 2026. How scammers use ads to target you on trusted websites. [accessed 1 May 2026].

[179] [✂] response to our formal information request issued 26 June 2025.

[180] ABI response to 2024 Call for Evidence, p.26; Cifas response to 2024 Call for Evidence, p.1; Sparkninety, 2022. Online Advertising Programme Market Insights. [accessed 13 March 2026]; Which? response to 2024 Call for Evidence, pp.3 to 5; Which?, 2025. How to spot and report scam search engine adverts. [accessed 11 March 2026]; Which?, 2025. Scammers are hiding behind Google's 'click-to-call' ads. [accessed 9 February 2026]; Which?, 2025. Scammers buy Google ads to con shoppers with a fake Costco website. [accessed 9 February 2026].

different from what a user would expect of a legitimate business's advertisement,[181] for example, by including spelling errors.

Investment and cryptocurrency advertisements

4.39 Investment and cryptocurrency fraudulent advertisements are typically seen on social media platforms,[182] and tend to offer high or guaranteed returns to attract users.[183] These advertisements also often feature fake celebrity endorsement and the use of AI and deepfakes.[184] Additionally, where an advertiser advertising an investment product is doing so without FCA authorisation, this is a sign that the content may be an investment scam.[185]

Use of GenAI and deepfakes

4.40 As mentioned in the sub-section 'Tools and techniques used in fraudulent advertising', GenAI is a commonly used tool in fraudulent advertising. It can be used, for example, to produce deepfakes that are used in advertisements that feature well-known figures to falsely act like they are promoting a product or service, or to draw attention to a fake news story as a form of clickbait. GenAI can also be used to recreate legitimate advertisements, and evidence shows that bad actors can use GenAI to slightly tweak the images or text from legitimate brands' advertisements to deceive users into thinking they are interacting with an advertisement from that brand.[186]

Exaggerated, attention-grabbing and pressure-inducing content

4.41 Fraudulent advertisements often rely on exaggerated, sensationalist or unrealistic claims designed to capture attention and prompt quick decisions. These can include high-return promises, urgency-inducing calls to action, or offers that appear too good to be true.[187] This might include language like "Only for 24 hours!", "Last few remaining!",[188] [✂][189] or "secure your retirement".[190]

4.42 Research shows that users are often drawn to advertisements that grab their attention, with two thirds of UK users that have interacted with potentially fraudulent advertisements saying they were extremely (31%) or moderately (35%) attention-catching.[191] These techniques frequently intersect with other forms of deception set out in this section, such

---

[181] Stop! Think Fraud, no date. How to spot a fake online advert. [accessed 9 February 2026]; Which?, 2025. How to spot and report scam search engine adverts. [accessed 11 March 2026].
[182] Cifas response to 2024 Call for Evidence, p.1; FCA, 2026. Crypto investment scams. [accessed 20 March 2026].
[183] Cifas response to 2024 Call for Evidence, p.1; Revolut (confidential) response to 2024 Call for Evidence, p.6; Sparkninety, 2022. Online Advertising Programme Market Insights. [accessed 13 March 2026]; Which?, 2023. Toward a future without fraud. [accessed 6 February 2026].
[184] ASA, 2026. A year in scams: 2025 update. [accessed 9 February 2026]; ASA response to 2024 Call for Evidence, p.4; Cifas response to 2024 Call for Evidence, p.1; Sparkninety, 2022. Online Advertising Programme Market Insights. [accessed 13 March 2026]; The Bureau of Investigative Journalism, 2024. Doctored Footage and Hijacked Accounts. [accessed 6 February 2026].
[185] See Volume 3, Section 3 'Preventing Fraudulent Financial Services Advertising', where we explain the financial services offences in more detail.
[186] SnapDragon, 2025. 10 Ways Fake Ads Are Targeting Your Customers. [accessed 17 February 2026].
[187] Stop! Think Fraud, no date. How to spot a fake online advert. [accessed 9 February 2026]; Which?, 2023. Toward a future without fraud. [accessed 6 February 2026].
[188] Stop! Think Fraud, no date. How to spot a fake online advert. [accessed 9 February 2026].
[189] [✂] response to our formal information request issued 26 June 2025.
[190] Which?, 2024. We exposed a global AI scam. [accessed 10 February 2026].
[191] Ofcom, 2026. Online paid-for advertisements research.

as the use of celebrities and brands, which further increases credibility and draws users into engaging with fraudulent advertisements.

Cloaking

4.43 Evidence indicates that bad actors may 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.[192]

Advertising account risky characteristics

Suspicious behaviour

4.44 There are various advertising account behaviours that may point towards them posting fraudulent advertisements, including:

- **Account details:** Accounts that post fraudulent advertisements might share the same or similar usernames, photos, bios and contact information.[193] Accounts may also undergo profile changes before beginning to post fraudulent advertisements.[194]
- **Account activity:** Accounts may have little or no activity before beginning to post fraudulent advertisements.[195] Some may produce 'filler content' featuring the same or similar text and content as posted by other accounts within a fraudulent network.[196] Accounts that post fraudulent advertisements might also follow or friend multiple accounts at once,[197] and they may post abnormal volumes of advertisements.[198]
- **Behaviour at sign-up:** Rapid account creation might signal that the account will post fraudulent advertising content.[199]
- **Abnormal patterns:** Accounts that post fraudulent advertisements might have irregularities in their behaviour. For example, there might be irregularities in their targeted locations, age or genders;[200] changes in their targeted audiences;[201] or mismatches between advertisements and the advertiser's stated purpose.[202] These advertising accounts may also edit or swap the content of paid-for advertisements they have placed, such as text or images.[203]

---

[192] ASA response to 2024 Call for Evidence, p.4; Confiant, no date. Malvertising attack matrix. [accessed 5 February 2026]; [✂] response to our formal information request issued 26 June 2025; Sparkninety, 2022. Online Advertising Programme Market Insights. [accessed 13 March 2026]; [✂] response to our formal information request issued 26 June 2025.
[193] Reset Tech, 2025. The Dormant Danger. [accessed 6 February 2026].
[194] [✂] response to our formal information request issued 26 June 2025.
[195] Reset Tech, 2025. The Dormant Danger. [accessed 6 February 2026]; [✂] response to our formal information request issued 26 June 2025.
[196] Reset Tech, 2025. The Dormant Danger. [accessed 6 February 2026].
[197] [✂] response to 2024 Call for Evidence, [✂].
[198] [✂] response to our formal information request issued 26 June 2025.
[199] [✂] response to our formal information request issued 26 June 2025.
[200] [✂] response to our formal information request issued 26 June 2025.
[201] [✂] response to our formal information request issued 30 January 2026.
[202] [✂] response to our formal information request issued 26 June 2025.
[203] Ofcom and Integrity Institute, 2026. Fraudulent advertising and account integrity; [✂] response to our formal information request issued 26 June 2025.

- **Advertising spend patterns:** Accounts that post fraudulent advertisements might display dramatic changes in advertising budgets or other behaviours such as new payment methods being added or an increase in failed payments.[204]

Impersonation through accounts

4.45 Fraudsters can also impersonate brands, organisations or public figures through the accounts that post paid-for advertisements.[205] Evidence suggests that GenAI will further enable bad actors to create convincing impersonated accounts.[206]

Impact of fraudulent advertising

Impact on individuals

4.46 Fraudulent advertising can have a large impact on individuals, and one stakeholder told us that they frequently hear from individuals who have suffered "significant harm" because of it.[207] Under section 234 of the Act, 'harm' means physical or psychological harm. We therefore refer to 'impacts' here rather than 'harm' as we include effects from fraudulent advertisements other than just physical and psychological harm.[208]

4.47 One kind of impact individuals can experience from fraudulent advertising is financial[209] loss.[210] A stakeholder told us that "the financial harm caused by fraudulent advertising can range from relatively inconsequential low value to life changing sums".[211] Ofcom research showed that 26% of respondents reported financial losses after interacting with a fraudulent advertisement, with 18% losing less than £100, 6% losing £100 to £999, 2% losing £1,000 to £9,999 and 1% losing £10,000 to £19,999.[212] Money Saving Expert (MSE) shared that victims reported losing over £20 million to advertisements impersonating Martin Lewis in 2022 to 2023, including an individual loss of £500,000.[213] A report from Juniper research also indicates that financial losses associated with 'scam ads' are potentially increasing.[214]

---

[204] [✂] response to our formal information request issued 30 January 2026.
[205] Meta, 2025. Adversarial Threat Report. [accessed 24 March 2026]; MSE response to 2024 Call for Evidence, p.25; Ofcom and Integrity Institute, 2026. Fraudulent advertising and account integrity; Ryan, J., 2025. TikTok removes AI weight loss ads from fake Boots account, BBC, 23 December. [accessed 11 March 2026]; UK Finance response to 2024 Call for Evidence, p.20.
[206] Ofcom and Integrity Institute, 2026. Fraudulent advertising and account integrity.
[207] MSE response to 2024 Call for Evidence, p.26.
[208] However, we still refer to 'harm' where we are quoting or referencing evidence from others, who may not have taken into account section 234 of the Act in their use of the term.
[208] MSE response to 2024 Call for Evidence, p.26.
[209] We have considered the financial impact of fraudulent advertisements as evidence shows that financial losses are a common effect of fraudulent advertisements, and because evidence shows that financial losses can lead to psychological harm in some instances (see paragraph 4.48).
[210] ABI response to 2024 Call for Evidence, p.26; BILETA response to 2024 Call for Evidence, p.34; Cifas response to 2024 Call for Evidence, p.2; Innovate Finance response to 2024 Call for Evidence, pp.9 and 10; Middle Tech Coalition (formerly Mid Size Platform Group) response to 2024 Call for Evidence, pp.5 and 6; MSE response to 2024 Call for Evidence, p.27; Which? response to 2024 Call for Evidence, p.2.
[211] ABI response to 2024 Call for Evidence, p.26.
[212] Ofcom, 2026. Online paid-for advertisements research.
[213] MSE response to 2024 Call for Evidence, p.27.
[214] Note that this research refers to 'scam ads on social media', which it defines as "a deceptive paid post that misleads users into giving money, personal information, or account access by falsely advertising products,

4.48 Individuals can also suffer significant non-financial impacts from fraudulent advertising.[215] Ofcom research found that, of those who lost money to fraudulent advertising, over half (54%) said it had an immediate impact on their mental well-being, and a third (33%) said the impact was long-term.[216] MSE told us that victims of fraudulent advertising can feel that their lives are ruined and, in the most extreme cases, can report feeling suicidal.[217] This is consistent with evidence that shows the health impacts of fraud more widely. A study by The Police Foundation found that 92% of those who had experienced fraud reported experiencing at least one health symptom as a result, with 58% feeling worried, 57% experiencing stress, 52% worrying about being victimised again, 46% experiencing emotional distress and 18% experiencing depression.[218] Additionally, the study found that 58% of victims reported experiencing a physical health symptom as a consequence of fraud.

4.49 We highlighted in our Illegal Harms Register that fraud victims encountered many challenges in their everyday lives.[219] These include anxiety and shame that prevents them from going to work or functioning in society; being cautious and wary online; and losing confidence in decision-making, feeling disappointed in themselves and becoming less trusting of others. This is supported by BILETA, who told us that fraudulent advertising can result in self-blame and a loss of confidence, as well as inconvenience and loss of time. Other impacts include damage to relationships, the need to take time off work, the desire to avoid social situations and even the loss of employment.[220]

4.50 As stated in 'Scale of fraudulent advertising', the emotional impacts of fraudulent advertising can also lead to under-reporting, which can make it difficult to understand its true impact. BILETA noted that for some victims, the potential negative perceptions associated with being a victim of online fraud, as well as the shame and emotional impacts suffered as a result, can prevent them from reporting the crime.[221]

services, or investment opportunities". Source: Juniper Research and Revolut, 2026. Protecting Users from Scam Ads. [accessed 13 February 2026].

[215] ABI response to 2024 Call for Evidence, pp.26 and 27; AGENCY response to 2024 Call for Evidence, p.9; BILETA response to 2024 Call for Evidence, p.34; Cifas response to 2024 Call for Evidence, p.2; The Cyber Helpline response to 2024 Call for Evidence, p.27; Innovate Finance response to 2024 Call for Evidence, pp.9 and 10; Middle Tech Coalition (formerly Mid Size Platform Group) response to 2024 Call for Evidence, pp.5 and 6; MSE response to 2024 Call for Evidence, pp.26 and 27; UK Finance response to 2024 Call for Evidence, p.17; Which? response to 2024 Call for Evidence, p.2.

[216] Ofcom, 2026. Online paid-for advertisements research.

[217] MSE response to 2024 Call for Evidence, pp.26 and 27.

[218] The study was conducted with victims of fraud in two neighbouring police force areas in England and Wales. The sample included all victims reported to or identified by police during June–September 2024. Victims assessed by police as having greater need were likely to be over-represented in the sample. Respondents were asked to select from a list of health symptoms they had experienced as a result of becoming a victim of fraud. The Police Foundation, 2026. Invisible harms: Understanding the hidden health impact of fraud. [accessed 25 March 2026].

[219] December 2024 Statement, Illegal Harms Register, p.241; See also Ofcom, 2023. Executive Summary Report: Online Scams & Fraud Research.

[220] BILETA response to 2024 Call for Evidence, p.34.

[221] Ibid.

Vulnerability

4.51 Evidence highlights that there is no set profile for victims of fraud.[222] A report by the Victims' Commissioner highlighted that vulnerability to fraud can stem from a wide spectrum of factors, such as age, life events, socio-economic classification, relationship status, ethnicity and prior victimisation. The report noted that it is usually the interplay of multiple factors that increases vulnerability to harm, but that a diverse range of people fall victim to fraud.[223]

4.52 Other evidence supports this, showing that vulnerability to fraud cannot be defined by demographics but may instead be based on situational and transient factors. Stakeholders and available evidence have noted that users may fall victim to scams when they are suffering from stress or serious emotional strain,[224] or when they are struggling financially.[225] The specific vulnerabilities arising from such situations can be targeted by fraudsters in the advertising space, with one stakeholder noting that by targeting keywords such as 'mortgage' and 'investment', bad actors are able to reach those looking for similar services and who therefore may be less likely to "question the truth of the ads which are put to them".[226]

4.53 Beyond situational and transient vulnerability, evidence indicates that individuals who have experienced mental health conditions are three times more likely than those who had never experienced a mental health problem to fall victim to an online scam (23% vs 8%).[227] The Money and Mental Health Policy Institute report also noted that individuals experiencing mental health conditions can find it difficult to spot scams and avoid losing money or personal information. The report also found that the impact of fraud can be more severe, as smaller financial losses can be damaging for these individuals who are more likely to be living on lower incomes or in problem debt.[228]

4.54 Evidence also shows that people who have already fallen victim to fraud are more susceptible to secondary attacks,[229] and there is some evidence to suggest a link between those who report a high personal impact of fraud and being a prior victim.[230] As described

---

[222] Brookes, A. and Norris, G., 2021. Personality, emotion and individual differences in response to online fraud, cited in BILETA response to 2024 Call for Evidence, p.34; MSE response to 2024 Call for Evidence, p.27; Which? response to 2024 Call for Evidence, p.2.
[223] The research draws on data from the 2017/18 and 2018/19 Crime Survey for England and Wales (CSEW). Victims' Commissioner, 2021. Who suffers fraud? [accessed 10 February 2026].
[224] Which? response to 2024 Call for Evidence, p.2.
[225] Research was conducted in August 2020. Pay.UK, 2022. All Aboard – Improving the payments system for financially vulnerable people. [accessed 27 March 2026].
[226] BILETA response to 2024 Call for Evidence, p.37.
[227] Figures on relative likelihood are from a nationally representative survey of UK online adults aged 18+ conducted in August 2020. Additional findings are based on a survey of the Institute's Research Community (n=340), a self-selecting sample of individuals with lived experience of mental health problems, conducted in July 2020. Money and Mental Health Policy Institute, 2020. Caught in the web: Online scams and mental health. [accessed 12 March 2026].
[228] Money and Mental Health Policy Institute, 2020. Caught in the web. [accessed 12 March 2026].
[229] The Cyber Helpline response to 2024 Call for Evidence, p.19; Victims' Commissioner, 2021. Who suffers fraud? [accessed 10 February 2026].
[230] The Police Foundation, 2018. More than just a number: Improving the police response to victims of fraud. [accessed 10 February 2026]; Victims' Commissioner, 2021. Who suffers fraud? [accessed 10 February 2026].

by a stakeholder, fraudsters can offer to help a victim recuperate their funds, and then take further advantage of the victim's situation.[231]

4.55 While vulnerability to fraudulent advertising cannot be defined by age alone, evidence relating to age can help to illustrate how vulnerability can arise in different ways and that no one age group is immune to fraudulent advertising. For example, while one stakeholder told us that older adults may be more vulnerable to fraudulent advertising,[232] other research showed that young adults aged between 18 and 24 are more likely to lose money to it.[233] A stakeholder told us that users above the age of 55 may be more likely to be targeted by investment scams relating to pensions through fraudulent advertisements, while those aged under 35 may be more likely to be targeted with cryptocurrency scams.[234] Additionally, people aged 65 and over have been found to be the most likely to fall victim to computer-related frauds.[235] Ofcom research showed that those aged 16-44 were more likely to be confident in their abilities to identify scams but did not respond appropriately to an email scam scenario.[236]

4.56 Children are also vulnerable to fraudulent advertising. Evidence suggests that they are more susceptible to advertising in general,[237] and children under 12 are not yet capable of critically evaluating advertising.[238] Additionally, Ofcom research found that only 42% of children were able to recognise paid-for advertising on search engines.[239] BeScamAware also highlights that children and teens often lack the experience to identify scams.[240] Evidence also showed that 46% of 8- to 17-year-olds say they have been scammed online (through online fraud more generally), with 9% of 8- to 17-year-olds reporting having lost money.[241] The impact of fraud on children can also be significant. The same study found that many children felt angry and annoyed (47%), upset or sad (39%), worried or stressed (31%), or embarrassed (28%) after falling victim to fraud. Children may also under-report fraud, with 47% saying that "they believe embarrassment is the top barrier to this". Other obstacles to reporting include the feeling that it is their fault and they will be blamed (41%), as well as the worry that they will get into trouble (40%).[242]

---

[231] ABI response to 2024 Call for Evidence, p.27.
[232] AGENCY response to 2024 Call for Evidence, pp.6 and 9.
[233] Ofcom, 2026. Online paid-for advertisements research.
[234] Cifas response to 2024 Call for Evidence, p.1.
[235] Victims' Commissioner, 2021. Who suffers fraud? [accessed 10 February 2026].
[236]. The scam scenario was an email delivery scam. Twenty per cent of those UK online adults aged 16 to 34 and eighteen percent of those aged 35-44 felt confident in their ability to detect scams but did not respond appropriately to the scam scenario. Source: Ofcom, 2026. Adults' Media Use and Attitudes Report.
[237] American Psychological Association, 2004. Report of the APA Task Force on Advertising and Children. [accessed 9 February 2026]; Rozendaal, E. and Bujizen, M., 2022. Children's vulnerability to advertising: an overview of four decades of research (1980s–2020s). [accessed 9 February 2026].
[238] Rozendaal, E. and Bujizen, M., 2022. Children's vulnerability to advertising: an overview of four decades of research (1980s–2020s). [accessed 9 February 2026].
[239] Forty-two per cent of UK children aged 8 to 17 who used search engines were able to identify, in the given scenario, that the top search results appeared because they were advertisements. Ofcom, 2026. Children and Parents: Media Use and Attitudes Report.
[240] BeScamAware, 2024. How to Talk to Children and Teens About Online Scams. [accessed 1 June 2026].
[241] Research was conducted online from September to October 2024 with a sample of 2,013 children aged 8–17. UK Safer Internet Centre, 2025. Almost half of 8 to 17-year-olds have been scammed online. [accessed 9 February 2026].
[242] Ibid. [accessed 9 February 2026].

4.57 Taken together, the available evidence does not provide a definitive answer as to which age groups are more susceptible to fraudulent advertising. However, it does clearly illustrate that a broad range of age groups may be vulnerable to fraudulent advertising, albeit users of different ages might be vulnerable in slightly different ways.

Wider impacts

4.58 Fraudulent advertising can also have impacts on businesses and industry. Evidence shows that fraud can undermine the trust people have in institutions and in the form of communication that enabled the fraud, as well as effects on the market and legitimate businesses.[243] Small and micro-businesses may be more likely to be affected, as their brands are less likely to be well known and therefore may rely more on the need for trust from users. Research by Which? supports this, as it showed that many users who had experienced online scams shifted towards buying from trusted retailors and established brands, which risks market concentration and squeezing smaller or newer businesses.[244]

4.59 Fraud can lead to victims disengaging with sites or services, and GASA state that 60% of people in the UK expressed reduced confidence in using the internet due to fraud.[245] This can have negative consequences for legitimate businesses that rely on online user engagement.

4.60 Two stakeholders highlighted that fraudulent advertising could lead to a distrust of new digital products and services and payment options. They said that this could damage the UK's reputation as a safe place to invest in fintech and financial services more generally.[246]

4.61 We heard from a stakeholder that brands that are impersonated through fraudulent advertising can often suffer damage to their corporate reputation as well as the unquantified financial costs of responding to innocent victims who believed they were transacting with the real company.[247] Businesses and organisations report significant impacts from impersonation and can encounter difficulties in reporting, resulting in repeated attempts to alert services and delays in fraudulent content being taken down.[248]

4.62 Evidence indicates that businesses can find the process of reporting fraudulent advertising to be cumbersome and inconsistent.[249] Small and medium-sized businesses – particularly those with lower advertising spend – highlighted that without access to a dedicated account manager, it can take significantly longer for problematic content to be reviewed and taken down, increasing the potential impact on their operations.

4.63 Fraudulent advertising can also have wider impacts by being used to fund criminal activity. For example, evidence suggests that bad actors use fake job advertisements to recruit money mules, who are then used to transfer funds between accounts as part of a

[243] Sentencing Council, 2013. Research on Sentencing Online Fraud Offences. [accessed 9 February 2026].
[244] Which?, 2026. The ripples of scams: impact on UK consumer behaviour online. [accessed 17 March 2026].
[245] GASA, 2024. Scammers Steal £11.4 Billion from Britons in 1 Year. [accessed 9 February 2026].
[246] Innovate Finance response to 2024 Call for Evidence, p.10; Revolut response to 2024 Call for Evidence, p.4.
[247] Cifas response to 2024 Call for Evidence, p.2.
[248] BBC response to 2024 Call for Evidence, p.5; Ofcom, 2026. Online advertising pathways: qualitative research report.
[249] Ofcom, 2026. Online advertising pathways: qualitative research report; Ofcom, 2026. Behavioural Audit of Services with Advertisement Functionality.

laundering process. This activity in turn facilitates other serious crimes such as terrorism, drug trafficking and people smuggling.[250]

4.64 More general evidence on the impacts of fraud supports this link to other forms of criminal activity. Written evidence submitted by Professor Nic Ryder to the Home Affairs Committee indicates that online fraud has been used to fund acts of terrorism.[251] Another report links cyber-enabled fraud with organised crime and human trafficking.[252] UK Finance further highlights that the connections between fraud, organised crime and terrorism are under-reported within the public domain but pose a significant and growing threat to the UK's national security.[253]

[250] Cifas, 2021. Money mule recruiters use fake online job adverts to target 'Generation Covid'. [accessed 3 June 2026].
[251] The online fraud referenced in the written evidence encompasses several forms, including romance fraud and the use of fake or fraudulent websites. Source: Nic Ryder, 2023. Written Evidence Submitted by Professor Nic Ryder (Cardiff University). [accessed 26 May 2026].
[252] Financial Action Task Force, Interpol, Egmont Group, 2023. Illicit Financial Flows from Cyber-Enabled Fraud. [accessed 26 May 2026].
[253] UK Finance, 2023. Written evidence submitted by UK Finance. [accessed 26 May 2026].

5. Our approach to developing Codes measures

The Online Safety Act places additional duties on providers of Category 1 and 2A services under sections 38 and 39 of the Act in relation to fraudulent advertising.

Codes of Practice are an important policy tool which Ofcom uses to get providers to take steps to tackle fraudulent advertising. Our proposed measures aim to promote this change in three key ways:

- **stop fraudsters posting fraudulent advertisements in the first place;**
- **improve the speed at which fraudulent advertisements are detected; and**
- **ensure swift action, once detected, to remove fraudulent advertisements.**

This section gives an overview of how we have approached developing our draft Codes. It also addresses how we have approached a number of specific considerations relevant to the fraudulent advertising context.

1. We have taken a layered approach to designing the draft Codes.

We consider there is no single intervention that can ensure UK users are adequately protected from fraudulent advertising. This is due to the scale of fraudulent advertising on in-scope services, and the way fraudsters continually adapt their tactics to evade detection.

We have therefore sought to tackle fraudulent advertising at different layers. We have placed significant emphasis on **account level interventions**, to stop fraudsters advertising from the outset and to address the scale and speed at which fraudulent advertising happens. We have then proposed further measures, in particular on moderation and reporting, to ensure that those fraudulent advertisements that make it through, are **detected and removed**.

2. We have prioritised safety by design when designing the draft Codes.

We consider effective **safety by design**, the practice of embedding protections into service features, systems and governance from the outset, is central to providers' actions to comply with their duties under the Act.

Our package of proposals emphasises how important this is, with our proposed **governance measures** (to ensure sufficient oversight and accountability for efforts to tackle fraudulent advertising risks), **fraud indicator assessment** (so providers understand how harm manifests, the material risks associated with content and accounts, and use these insights to better apply other mitigations), **strengthening account integrity** (to prevent fraudulent actors accessing advertising systems), and the robust **testing of AI advertisement generation tools** (to identify and address vulnerabilities they identify).

3. We have carefully designed measures that are proportionate for the range of service providers in scope.

We have carefully designed our proposed measures, to ensure they are appropriate for in-scope service providers. In doing so, we have considered a range of important factors.

We have considered, for example, both the severity of harm posed by fraudulent advertising and the degree of control providers have over the placement of advertisements. Our understanding of the scale and impact of fraudulent advertising in the UK underpins our approach to designing measures,

ensuring that the benefits of proposed measures are appropriately balanced against their potential costs and impacts. We also recognise that while most Category 1 and 2A services are likely to have substantial control over the placement of advertisements, particularly where they operate owned and operated advertising supply chains, there may be more complex scenarios involving third-party intermediaries where control is reduced. Our proposed advertising intermediaries measure[254] accounts for this by providing an alternative pathway to compliance.

Fraudulent advertising is a particularly adversarial space, and technology and best practice evolve at pace. As such, we have taken a balanced approach to measure design, setting enough detail for providers to be clear on the actions they need to take, and adding enough flexibility where it is needed to help ensure that our proposals are sufficiently future proofed.

We will continue our iterative approach to designing Codes we have set out in previous consultations and statements. This means proposing a package of measures we consider will give us a strong foundation on which to build over time.

Consultation question

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

What this section does

5.1 This section outlines our proposed approach to developing our proposed measures for inclusion in the draft Fraudulent Advertising Codes of Practice (the Codes)[255].

5.2 The section describes the purpose of our online safety Codes of Practice as outlined in the Online Safety Act 2023 ('the Act') and our strategy and iterative approach to Codes. It then discusses the following aspects of our approach:

a) our approach to developing and impact assessing proposed measures; and
b) our approach to addressing specific considerations relevant to the fraudulent advertising context.

The Online Safety Act 2023 and the Codes

5.3 The Act is a set of laws designed to protect children and adults online. It puts a range of duties on providers of user-to-user and search services and sets out their responsibilities for UK users' safety. The Act also imposes new duties on providers of Category 1 and 2A services (service providers) under sections 38 and 39 of the Act in relation to fraudulent advertisements (the fraudulent advertising duties). For a summary of the duties see Volume 1, Section 2, 'Introduction' and a further explanation in Annex 2, 'Legal framework'.

5.4 The Act places a requirement on us to prepare and issue Codes, which are a package of measures recommended for service providers to comply with their fraudulent advertising duties. We can only recommend measures which relate to the design, operation and use of a Category 1 or 2A service in the UK (or as it affects UK users of the service).[256] We must

[254] See Volume 2, Section 2, 'Advertising intermediaries'.
[255] The Codes are made up of two sets of draft Codes, one for proposed measures applicable to Category 1 user-to-user services and one for proposed measures applicable to Category 2A search services.
[256] Paragraph 11 of Schedule 4 to the Act. The fraudulent advertising duties only apply to Category 1 and 2A services with links to the UK as defined in section 4 of the Act. They also only apply to the design, operation and use of the service in the UK: see sections 38(7) and 39(7) of the Act.

also ensure that the measures described in the Codes are compatible with the pursuit of the list of online safety objectives set out in Schedule 4 to the Act.[257]

5.5 The Act sets out that Ofcom must consider the appropriateness of the measures we recommend to different kinds and sizes of services and to providers of differing sizes and capacities.[258] We must also have regard to the principles that:

- providers must be able to understand which measures apply in relation to their service(s);
- the measures must be sufficiently clear, and at a sufficiently detailed level, that providers understand what they entail in practice;[259] and
- the measures must be proportionate and technically feasible.[260]

5.6 Under the Communications Act 2003 (the 2003 Act), we are also required to conduct impact assessments when preparing a Code or amendment to a Code, including an assessment of the impact on small and micro-businesses.[261]

5.7 We set out our approach to impact-assessing our proposed measures in paragraphs 5.47 to 5.49, including our impact assessment criteria.

5.8 The Codes act like a 'safe harbour', meaning that service providers who implement all applicable measures in the Codes will be treated as complying with their relevant duties under the Act.[262] This consultation details the draft measures we propose providers of Category 1 and 2A services should implement to be treated as compliant with the fraudulent advertising duties.

5.9 Service providers do not need to follow our Codes and may seek to comply with their duties by taking what the Act calls 'alternative measures'. Where providers take alternative measures, they must be able to show how those measures ensure they are operating their services in compliance with the fraudulent advertising duties set out in sections 38 and 39 of the Act.

5.10 We have produced two sets of draft Code measures for consultation. One document contains draft measures applicable to Category 1 services, see Annex 4 'Draft code for user-to-user services' and the other, Category 2A services, see Annex 5, 'Draft code for search services'.

---

[257] Paragraph 3 of Schedule 4 to the Act. The online safety objectives for regulated user-to-user services are set out in paragraph 4 and for regulated search services in paragraph 5.
[258] Paragraph 1 of Schedule 4 to the Act.
[259] Paragraph 2 of Schedule 4 to the Act. Paragraph 2 sets out other additional principles that we must take into account when preparing a draft of a code of practice (see Annex 2, 'Legal framework' for further details).
[260] Measures that are proportionate or technically feasible for providers of a certain size or capacity, or for services of a certain kind or size, may not be proportionate or technically feasible for providers of a different size or capacity or for services of a different kind or size. See paragraph 2(c) of Schedule 4 to the Act.
[261] Section 7 of the 2003 Act, as amended by section 93 of the Act.
[262] Section 49(4) of the Act: "A provider of a Category 1 service or a Category 2A service (or a provider of a service which is both a Category 1 service and a Category 2A service) is to be treated as complying with a duty set out in Chapter 5 if the provider takes or uses the measures described in a fraudulent advertising code of practice which are recommended for the purpose of compliance with the duty in question."

Our strategy

Approach to online safety

5.11 Under the Act, Ofcom's role is to make online services safer by making sure providers of regulated services have effective systems in place to protect UK users from harm. We have a number of regulatory tools to help us achieve this goal, including supervisory, enforcement, transparency and policy tools.[263]

5.12 One important policy tool is our Codes of Practice. These set out what we consider providers should do to meet their duties under the Act. In some cases, our proposals broaden the application of existing good practice to other providers. In other cases, where we consider it necessary for providers to meet the duties in the Act, our proposals go beyond current industry best practice.

5.13 The services in scope of the fraudulent advertising duties are some of the most widely used user-to-user and search services.[264] Therefore, what is proportionate to recommend to these providers to comply with the fraudulent advertising duties may be more onerous and costly than in cases where duties apply to the full range of regulated online services including small and micro-businesses.[265]

5.14 Some of our Codes of Practice are already in force, including our Illegal Content Codes of Practice.[266] These Codes include recommendations for providers of in-scope services to meet their illegal content duties to identify and take action against fraudulent user-generated content and search content.[267]

5.15 This consultation will build on our existing recommendations about fraudulent user-generated content and search content by proposing a range of measures to ensure providers of Category 1 and 2A services take action to address fraud in paid-for advertising. This includes carrying forward a number of cross-cutting measures from the Illegal content Codes and then layering these with a range of fraudulent-advertising-specific measures. We consider the approach we have taken best ensures coherence with the existing framework, whilst also addressing the distinct ways fraud manifests in online advertising and the scope of the fraudulent advertising duties under the Act.[268]

---

[263] For more about how Ofcom drives change, see Ofcom, 2025. Online Safety in 2025: Summary of the technology sector's response to the UK's new online safety rules.

[264] They have at least 7 million average monthly active UK users. See The Online Safety Act 2023 (Category 1, Category 2A and Category 2B Threshold Conditions) Regulations 2025, paras 3(1) and 4(a).

[265] For more on impacts on small and micro-businesses see Volume 1, Section 6, 'Combined impact assessment'.

[266] The Illegal Content Codes of Practice were published in December 2024 and came into force on 17 March 2025. We published our Consultation: Online Safety – Additional Safety Measures on 30 June 2025. It proposed a series of additional safety measures to further strengthen the Illegal content Codes, including wider use of automated technologies to detect fraud in user-generated content (among other harms) and user sanctions in respect of UK users who generate, upload or share fraud in user generated content (along with other harms). For more information on these and other published products, such as our Protection of Children Codes of Practice, see Volume 1, Section 2, 'Introduction'.

[267] Providers of in-scope user-to-user, search and combined services have duties under section 10 and section 27 of the Act, respectively, in relation to illegal content and priority illegal content. Priority illegal content includes content that amounts to an offence specified in Schedules 6 and 7 to the Act which includes the fraud etc. offences specified in section 40 of the Act.

[268] We explain the strategy behind adapting existing recommendations for cross-cutting systems and processes below under 'Approach to regulatory alignment' and the strategy for our advertising specific proposals in Volume 1, Section 1, 'Overview'.

5.16 We have been clear throughout the process of implementing the Act that our regulatory approach must be dynamic.[269] This is a pragmatic approach given the speed at which harm, technology and best practice evolve. We will work with our regulatory partners, law enforcement, government, and other stakeholders to ensure we continue to take action to keep UK users safe as far as appropriate and feasible within our remit as the regulator responsible for online safety.[270] These Codes will provide our first iteration for fraud in online paid-for advertising. We consider it to be a strong foundation on which to build over time, similar to our iterative approach for our illegal harms and protection of children regulatory products.

Approach to designing our fraudulent advertising proposals

5.17 In setting out our approach, we have sought to understand the scale and impact of fraudulent advertising, and current industry practices around mitigations for fraudulent advertising. In doing this, we have considered insights from stakeholders including both public and private sector stakeholders and civil society.[271] We have also gathered evidence from formal and informal information requests, commissioned reports and research,[272] and conducted desk research, among other activities.

5.18 From our engagement and wider evidence gathering, we understand that while providers have taken some steps to address fraudulent advertising, they are not going far enough, and are not adequately ensuring the protection of users.[273] Our Codes, and the threat of enforcement action and substantial fines for non-compliance, in conjunction with our wider regulatory toolkit, will provide an important catalyst for better practices across in-scope services.[274]

5.19 We consider there is no single intervention that can ensure UK users are adequately protected from fraudulent advertising. This is due to the magnitude of this harm and the

[269] We discussed our iterative approach to designing Codes in our December 2024 Statement on Protecting People from Illegal Harms Online. See Ofcom, 2024. Our approach to developing Codes measures, pp.12 and 13; We also discussed in our June 2025 Consultation. See Ofcom, 2025. Additional Safety Measures: Online Safety, pp.20 to 22.

[270] Online advertising systems are large, complex, and constantly evolving. The harms associated with them are equally varied. We set out information on the scale and impact of fraudulent advertising in Volume 1, Section 4, 'Causes and impacts of fraudulent advertising', along with some of the challenges for users experiencing advertising harms that fall outside the scope of the fraudulent advertising duties.

[271] This includes holding stakeholder engagement meetings, issuing formal requests for information under section 100 of the Act and undertaking other informal information gathering activities with service providers, other regulators, industry bodies and experts and others.

[272] This includes: Ofcom and Integrity Institute, 2026. Fraudulent advertising and account integrity: Expert insights on best practice; Ofcom, 2026. Online advertising pathways: qualitative research report; Ofcom, 2026. Online paid-for advertisements research; Ofcom, 2026. Behavioural audit of services with advertising functionality.

[273] Online fraudulent advertising is continuing to grow at exponential rates, along with the immense associated societal and individual harms. We set out the scale and impact of this issue in detail in Volume 1, Section 4, 'Causes and impacts of fraudulent advertising'. We set out the incentives on providers to not take adequate action to protect users from fraudulent advertising in Volume 1, Section 3, 'Online advertising ecosystem'.

[274] Ofcom 2024, How Ofcom approach enforcement (accessed 17 June, 2026).

way fraudsters continually adapt their tactics, exploiting new trends and technologies to target vulnerabilities among UK users.[275]

5.20 Therefore, we are proposing a layered approach to tackling fraudulent advertising. Specifically, we have designed measures to:

a) **Stop fraudsters posting fraudulent advertisements in the first place**. This includes our proposed measures on account checks and actions, immediate advertising bans on those who have posted fraudulent advertisements, and actions providers should take to prevent fraudsters from returning.[276]
b) **Improve the speed at which fraudulent advertisements are detected**. This includes our fraud indicator assessment (FIA)[277] (which helps services understand how fraudulent advertising manifests on their service), our proposed ad libraries measure and dedicated reporting channels measure,[278] and the proposal on the use of proactive technology that we are developing.[279]
c) **Ensure swift action, once detected, to remove fraudulent advertisements**. This includes ensuring providers resource, train and provide appropriate materials to individuals working in moderation, as well as our proposed measure to ensure swift removal of fraudulent advertisements.[280]

5.21 We have placed significant emphasis on account-level interventions. A number of expert stakeholders have indicated that account-level interventions are highly effective in addressing fraud. They have also emphasised that significant opportunities exist for service providers to enhance current practices and combat the increasing scale and speed of fraudulent advertising.[281]

5.22 We have carefully calibrated the degree of specificity and flexibility in our proposed measures. We have designed the measures to ensure they are specific enough for providers to understand what is expected of them, while also building in sufficient flexibility to help ensure they are appropriate for the full range of in-scope services and remain so over time.[282] Flexibility is particularly important, given the adversarial nature of fraudulent advertising.

5.23 We have aimed to design the measures to accommodate evolving perpetrator tactics, as well as allowing for the pace of digital change and advances in technology and best practice. Our proposals include measures to ensure that providers are actively assessing how fraud manifests on their service and that they put in place proper oversight and accountability structures to ensure their systems and processes work effectively in practice from the

[275] We set out more information on vulnerability in Volume 1, Section 4, 'Causes and impacts of fraudulent advertising' under the sub-heading 'Vulnerability'.
[276] For more information on our account integrity proposals see Volume 3, Sections 2 to 6.
[277] See Volume 2, Section 3, 'Fraud indicator assessment'.
[278] For more information on these proposals see Volume 4, Section 5, 'Ad libraries' and Volume 4, Section 4, 'Advertising complaints'.
[279] We understand that many large service providers use proactive technology to detect fraudulent advertisements and we plan to propose measures on this in Autumn 2026. Please see paragraphs 2.14 and 2.15 in Volume 4, Section 2, 'Advertising moderation' for more detail.
[280] For more information on our moderation proposals, see Volume 4, Section 2, 'Advertising moderation'.
[281] For further information on our account integrity measures, see Volume 3, Sections 2 to 6.
[282] This aligns with the principle set out at paragraph 2(b) of Schedule 4 to the Act, which Ofcom must have regard to when preparing a draft code of practice.

outset and over time. We set out more information on the combined impact of our package as a whole in our combined impact assessment.[283]

Safety by design

5.24 To effectively prevent users from encountering fraudulent advertisements, we consider that providers of Category 1 and 2A services need a mix of upstream and downstream measures. They should apply upstream 'safety by design' measures to reduce the likelihood of the service being used for fraudulent advertising, and downstream preventive and responsive measures to identify and remove those fraudulent advertisements that are still able to be encountered by users.

5.25 Safety by design measures include those that ensure a service is designed and operated, including in relation to its features and functionalities, in a way that proactively supports safer outcomes for users. Achieving better safety by design outcomes is an important part of compliance with the duties under the Act.[284] In this context it is important for providers to ensure that the systems and processes put in place to protect consumers against fraud are fully integrated into wider business governance and control frameworks.

5.26 In our Illegal content Codes and Protection of Children Codes of Practice we recommended a number of safety by design measures. We explained the importance of safety by design in relation to these Codes in the relevant statement documents.[285]

5.27 For this consultation, we have similarly considered the importance of safety by design practices when developing our proposals. Examples where our proposals ask for safety by design include:

a) Our FIA proposal, which sets out that service providers should assess how fraudulent advertising manifests on their service, will ensure providers have the relevant information they need to tailor controls, prioritise interventions, and continuously improve their approach based on identified risks and harms.[286]
b) Our account integrity proposals, which set out that services should carry out checks on accounts, implement account security and ban fraudsters from using advertising systems, will ensure upfront verification and ongoing checks where appropriate, ensure fraudulent actors are prevented from creating or taking over accounts, and reduce the opportunity for harm at the earliest stage of the process.[287]
c) Our testing advertisement generation tools (testing) proposal, which sets out that service providers should test and address vulnerabilities in their artificial intelligence (AI) advertisement generation tools in relation to fraudulent advertising, will ensure user safety is embedded into product development and ensure relevant tools are resilient to misuse before they are deployed and as they evolve.[288]
d) Our governance and accountability proposals, which set out that providers should ensure appropriate oversight for compliance activities to meet the duties under the Act, will ensure clear lines of accountability, regular reporting on fraudulent advertising

[283] See Volume 1, Section 6, 'Combined impact assessment'.
[284] See section 1(3)(a) of the Act.
[285] In our December 2024 Statement, Our Approach to developing Codes measures, paragraphs 1.48 to 1.50 and, in our April 2025 Statement on Protecting Children from Harms Online' in Our regulatory Approach, p. 23 and in Volume 4, throughout Section 9, 'Overview of Codes'
[286] For more information on this proposal, see Volume 2, Section 3, 'Fraud indicator assessment'.
[287] For more information on these proposals, see Volume 3, Sections 2 to 6.
[288] For more information on this proposal, see Volume 2, Section 5, 'Testing advertisement generation tools'.

concerns, and board or senior management oversight to ensure safety considerations shape product and business decisions from the outset.[289]

Enforcement

5.28 We expect the duties to come into force, 21 days after the Codes have passed through parliament.[290] We will, as part of our supervision activities, closely monitor the implementation of the Codes. In addition, once the duties come into effect, we will not hesitate to take enforcement action against providers should we become aware of potential breaches of the duties that expose UK users to significant risk of harm.[291]

5.29 We will take a reasonable and proportionate approach to enforcement, having regard to the lead times required to implement the measures. Once they come into force, we expect service providers to start taking action to come into compliance with the duties immediately and will hold them to account where they do not. In most cases, the lead times for implementing the measures we have set out should be small. If we were to enact the codes we have proposed in this consultation, we would therefore expect the majority of the measures to be in place shortly after the codes came into force. Our analysis suggests there are a small number of measures which are more complex and could require a little more time to implement. Specifically, we estimate that:

i) A first-time build of an ad library[292] could take around 6 months.
ii) It could take a new service up to three months to build enough data to undertake a robust FIA.[293]
iii) For a service without existing account checks[294] or financial services verification processes[295] it could take between three to six months to implement these measures.

5.30 We would only expect the slightly longer lead times for the three measures set out above to apply where service providers are deploying these functionalities for the first time. Where they are adapting existing ad libraries or account checks, we would expect the lead times to be materially shorter.

Approach to regulatory alignment

5.31 We consider it good practice to be mindful of opportunities to create regulatory alignment across our own products and with other jurisdictions, where it aligns with our policy objectives and is appropriate for the duties in the Act. Our priority is always the implementation of the Act as intended by Parliament and compliance with our duties under the Act, the 2003 Act and other principles of public law.

---

[289] For more information on these proposals, see Volume 2, Section 4, 'Governance and accountability'.
[290] We will aim to publish the Codes mid-2027. We expect the Codes to come into force 21 days after they complete their passage through Parliament. The fraudulent advertising duties start to apply to providers on the day on which the Codes come into force: section 51(5) of the Act.
[291] For more information please see our Enforcement Guidance, published as part of our December 2024 Statement, accessed 18 June 2026.
[292] For more information on our ad library proposal see Volume 4, Section 5.
[293] For more information on our FIA proposal see Volume 2, Section 3.
[294] For more information on our account checks proposal see Volume 3, Section 2.
[295] For more information on our financial services verification proposal see Volume 3, Section 3.

5.32 We consider such an approach helps to reduce unnecessary burden on providers of services that are in-scope of more than one of our regulatory products, and on service providers that are more likely to be operating across different geographic jurisdictions (such as those with large enough user bases to be categorised).

5.33 An example of this is our approach to considering requirements set out under the EU Digital Services Act (DSA) (EU)[296], including:

a) our consideration of the principles, functionalities and information categories included in Article 39 of the DSA[297] when proposing our measure on ad libraries. We set out the intersection with Article 39 and our proposed measure, and how this may impact costs, further in Volume 4, Section 5[298]; and
b) our consideration of the retention periods for record-keeping of risk assessments under the DSA[299] when proposing retention periods for record-keeping elements across our proposals.[300]

5.34 Our approach to align certain cross-cutting measures across Illegal content Codes and for this consultation, is another example of seeking opportunities for regulatory alignment. We consider our governance and accountability, terms of service and publicly available statements, advertising moderation and advertising complaints measures, to be essential building blocks for protecting users from harm online.[301] These types of measures provided a foundation on which more targeted harm-specific interventions were layered in our Illegal content Codes and Protection of Children Codes and now, provide a similar foundation for our draft Fraudulent Advertising Codes.

5.35 As far as appropriate and feasible for the fraudulent advertising duties and context, we have taken the approach to align our cross-cutting proposals with our Illegal Content Codes while ensuring they are appropriate for the fraudulent advertising context. We consider this creates the following benefits:

a) **Reducing compliance burden**. This helps external stakeholders realise efficiencies where it is possible to operate shared or connected systems and processes across content or harm types, and, reduces requirements for duplicative or piecemeal stakeholder engagement with consultations, where Codes can be updated or iterated more holistically.

---

[296] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)
[297] Article 39 requires VLOPs and VLOSEs to operate a public, searchable advertising repository.
[298] We set this out further under sub-heading 'Regulatory alignment' and 'Costs for adjusting an existing ad library'.
[299] Per Article 34, Risk assessment - the Digital Services Act (DSA), providers of very large online platforms and of very large online search engines shall preserve the supporting documents of the risk assessments for at least three years after the performance of risk assessments, and shall, upon request, communicate them to the Commission and to the Digital Services Coordinator of establishment.
[300] For more information on proposed measures with record-keeping steps, see, Volume 2, Section 2, 'Advertising intermediaries', Section 3, 'Fraud indicator assessment', Section 4, 'Governance and accountability', and Section 5, 'Testing advertisement generation tools'; Volume 3, Section 2, 'Account checks and actions', Section 3, 'Preventing fraudulent financial services advertising' and Section 5, 'Advertising bans'; and Volume 4, Section 4, 'Advertising complaints'.
[301] For more information on these proposals see Volume 2, Section 4, 'Governance and accountability'; and Volume 4, Section 2, 'Advertising moderation', Section 3, 'Terms of service and publicly available statements', and Section 4, 'Advertising complaints'.

b) **Regulatory certainty and clarity**. We promote readability and accessibility for external stakeholders by ensuring that measures with similar policy intent and compliance expectations are designed and explained consistently.
c) **Reducing risk of unintended consequences.** Alignment limits the likelihood of inconsistent or confusing user experiences of safety tools (for example, different recommendations for complaints tools across Illegal content Codes of Practice and our Fraudulent Advertising Codes, where it may not be possible for users to distinguish between paid-for advertising and user-generated content).

5.36 For more information on our proposals that are adapted from our Illegal content Codes of Practice see Volume 2, Section 4, 'Governance and accountability' and Volume 4, Section 2, 'Advertising moderation', Section 3, 'Terms of service and publicly available statements', and Section 4, 'Advertising complaints'.

Approach to record-keeping

5.37 To ensure that measures are effective and fit for purpose in meeting the fraudulent advertising duties, we have, where necessary, included record-keeping steps within the proposed measures. In particular, we consider record-keeping supports the following objectives:

a) **Ensuring appropriate governance.** Ensuring effective implementation of safety measures depends on clear oversight and governance.[302] Record-keeping supports this by providing a transparent audit trail of decisions taken, the rationale for them and how concerns have been addressed. It also allows organisations to monitor performance and trends. This enables appropriate scrutiny by senior management where needed, helps prevent retrospective re-characterisation of decisions, and supports meaningful review of measures and efforts towards evaluating and improving systems, including as part of the annual review process. We consider ensuring effectiveness of measures taken to protect users in practice, via record-keeping and scrutiny of these records, is a key part of compliance with the regime.
b) **Ensuring quality assurance and resilience of systems**. Maintaining appropriate records enables teams to understand what approaches have previously been tested, assess the effectiveness of changes, and iteratively improve mitigations over time. Record-keeping also reduces operational risk by preserving institutional knowledge and supporting continuity across teams despite organisational change or staff turnover. This is particularly important where measures have been designed to evolve in response to technological advancements (for example, our account checks and actions or testing measure),[303] changing fraudster tactics (for example, our FIA measure),[304] or changing relations with advertising intermediaries that are involved in the placement of paid-for advertising on a regulated service (for example, our advertising intermediaries measure).[305] We consider ensuring organisational capability to iterate and improve systems, via appropriate record-keeping, is a key part of addressing evolutions of fraud and technology and of ensuring ongoing compliance with the regime.

[302] See Volume 2, Section 4, 'Governance and accountability' for more detail on our governance and accountability proposals.
[303] See Volume 3, Section 2, 'Account checks and actions' and Volume 2, Section 5, 'Testing advertisement generation tools'.
[304] See Volume 2, Section 3, 'Fraud indicator assessment'.
[305] See Volume 2, Section 2, 'Advertising intermediaries'.

5.38 Where we propose record-keeping steps in measures, we generally propose a minimum retention period of three years. This is intended to provide sufficient continuity to support benefits mentioned in paragraph 5.37, while remaining proportionate and aligned with broader regulatory practice. This aligns with the approach we have taken in previous regulatory products[306] and aligns with the DSA (as set out in paragraph 5.33).

5.39 We set out more information on our rationale for our record-keeping proposals in the relevant measure sections.[307]

Approach to control and working with intermediaries

5.40 As set out in Volume 2, Section 2, 'Advertising intermediaries', all Category 1 and Category 2A services are in scope of the fraudulent advertising duties under the Act regardless of the pathway used to serve paid-for advertisements to users. Relatedly, the degree of control a provider has in relation to the placement of paid-for advertisements on the service is relevant in determining what is proportionate for the purposes of complying with the fraudulent advertising duties.[308]

5.41 Given this, we consider that it was Parliament's intent to acknowledge how degree of control may impact what is proportionate for the purposes of the fraudulent advertising duties, to account for intricacies that arise when third-party advertising intermediaries may be involved in the placement of paid-for advertisements on Category 1 or Category 2A services.[309]

5.42 We provide an overview of regulated services and the types of 'advertising pathways' they may use in Volume 1, Section 3, 'Online advertising ecosystem'. [310] Particularly, we note:

a) Providers can place paid-for advertisements using an 'owned and operated' supply chain,[311] where the supply chain is integrated with the service, or via an open-display supply chain,[312] which involves multiple advertising intermediaries operating in the open-display market.[313]

---

[306] Ofcom, 2025 Record-Keeping and Review Guidance.
[307] See, Volume 2: Section 2, 'Advertising intermediaries', Section 3, 'Fraud indicator assessment', Section 4, 'Governance and accountability', and Section 5, 'Testing advertisement generation tools'; Volume 3: Section 2, 'Account checks and actions', Section 3, 'Preventing fraudulent financial services advertising' and Section 5, 'Advertising bans' and Volume 4, Section 4, 'Advertising complaints'.
[308] Sections 38(5)(b) and 39(6)(b) of the Act.
[309] As set out in the explanatory notes to the Act, in reference to degree of control, "a Category 1 service may rely on third party intermediaries to display paid advertisements on its service, and will therefore have less control over measures to prevent posting of fraudulent adverts".
[310] See under sub-heading 'Overview of regulated services'. Advertising pathways refer to the systems and processes through which advertisements travel from advertisers or media agencies to the services where they are displayed. These pathways are complex and dynamic, varying between services. For more information on advertising pathways see paragraphs 3.16 to 3.40.
[311] An 'owned and operated supply chain' is vertically integrated with the service and owned by the service provider, allowing control over advertiser verification, ad moderation, and other mitigation measures. Intermediaries may be involved but are integrated within the provider-owned system. For more information see paragraphs 3.26 to 3.28.
[312] The open-display market involves multiple intermediaries such as demand-side platforms, supply-side platforms, ad exchanges, and others. Providers may have limited control over the ad placement process, which can complicate efforts to prevent fraudulent advertising, though they can still take certain actions (e.g. set parameters and blocklists). For more information see paragraphs 3.29 to 3.37.
[313] Providers may also engage in direct deals with advertisers. For more information see paragraphs 3.38 to 3.40.

b) The type of advertising supply chain used can have an impact on the degree of control a provider has over the placement of advertisements which, in turn, may have an impact on the safety mitigations a provider would need to put in place to address fraudulent advertising on categorised services.[314]

5.43 Providers could also have a mixture of paid-for advertisements from both an owned and operated supply chain and open-display supply chains, or a mixture of paid-for advertisements from different open-display supply chains. Therefore, the degree of control a provider has over the placement of different paid-for advertisements, and the application of measures, may differ across a single service.

5.44 We gathered evidence on the advertising supply chains used by many of the most widely used user-to-user and search services.[315] We understand that most categorised services will use owned-and-operated supply chains. In such instances, service providers would generally play an active role in all aspects of the advertising supply chain and therefore would be able to apply mitigations across that supply chain. On this basis, we consider it is unlikely there will be many situations where Category 1 and Category 2A service providers' degree of control over the placement of advertisements impacts their ability to implement the measures in the draft Codes.

5.45 Where a Category 1 or Category 2A service provider's degree of control over the placement of paid-for advertisements means they cannot apply a proposed measure,[316] we have proposed a proportionate path through which they can comply and remain in the safe harbour. We set out our expectations for these situations in Volume 2, Section 2, 'Advertising intermediaries'.

5.46 We note that the degree of control a provider has in relation to the placement of advertisements is not the only matter that the Act states is particularly relevant to determining what is proportionate for the purpose of complying with the fraudulent advertising duties. The Act also stipulates that the nature, and severity, of potential harm to individuals presented by different kinds of fraudulent advertisement is particularly relevant. We have taken both into account in designing our measures and set out a detailed discussion of the harm from fraudulent advertising in Volume 1, Section 4, 'Causes and impacts of fraudulent advertising' which serves as a foundation for our measures. We set out further information on our approach to assessing scale and impact of fraudulent advertising in the following sub-section from paragraph 5.47.

Approach to assessing measures via our impact assessment framework

5.47 When assessing the case for including a measure in the Codes, we consider the following core factors:

[314] For more information see paragraphs 3.27 to 3.28 and 3.35 to 3.37.
[315] We set this out in Volume 2, Section 2, 'Advertising intermediaries, in paragraph 2.3.
[316] This applies to all measures except those in Volume 2, Section 4 'Governance and accountability' and Section 5, 'Testing advertisement generation tools' and Volume 4, Section 3, 'Terms of service and publicly available statements'. We set out in each relevant measure section if and how the intermediaries measure may apply.

a) **Scale and impact of fraudulent advertising.** Our assessment of the scale and impact of fraudulent advertising in the UK provides us with an important foundation to contextualise the likely benefits of a proposed measure, and to balance those benefits against the potential rights and costs impacts. This helps us to determine what is proportionate for providers to comply with the fraudulent advertising duties. Under the Act, one of the factors relevant to proportionality is the nature, and severity, of potential harm to individuals presented by different kinds of fraudulent advertisement.[317] To avoid repetition, we have set out our evidence base on the scale and impact of fraudulent advertising in Volume 1, Section 4, 'Causes and impacts of fraudulent advertising'. Individual measure sections refer to this section to demonstrate how this evidence has been taken into account when considering a proposed measure. We also set out more information on scale and impact of fraudulent advertising in Volume 1, Section 6, 'Combined impact assessment'.
b) **Likely benefits.** In assessing the proportionality of a proposed measure, we have considered likely benefits and effectiveness of such a measure to reduce the incidence of UK users encountering fraudulent advertisements on a service. This includes assessing any evidence derived from current use of similar interventions by services, with particular focus on services with larger user bases (which is more likely to be relevant for Category 1 and 2A services). Such evidence is important in setting out why the measure is proportionate when balanced against the potential costs and human rights impacts. We set out more information on the combined benefits of our proposals in Volume 1, Section 6, 'Combined impact assessment'.
c) **Impacts and costs.** We have considered costs broadly, including direct costs to providers of implementing measures (for example, setting up and maintaining the measure) and indirect costs (for example possible knock-on effects of the measure). We have quantified the potential costs where possible.[318] Where relevant information to quantify costs is not available, we have instead described what we believe the nature of the costs may be, recognising that they are likely to vary by service. Where we have quantified costs, our estimates are based on the assumption that services would have to implement the measure from scratch or where existing regulation is in place, such as the Illegal content Codes of Practice (and, in some cases, the DSA), that services would adapt those measures for the fraudulent advertising context. For each measure and type of cost, rather than providing a single cost estimate, we have provided a range. This range reflects how costs are expected to vary with factors affecting the scope and complexity of the changes that providers will have to undertake to comply with their duties (for example the scale of advertising hosted on the service, the extent to which different services will be able to leverage their existing infrastructure and capability, and so on). We generally expect that for most measures, services hosting a smaller volume of advertisements and services with smaller user bases will likely incur costs closer to the lower bound of our estimates (unless otherwise specified). Our assessments of the impacts and costs on the services further consider the extent to which some services are likely to be already undertaking measures similar to our proposed measures and how this may reduce costs in practice. We set out more

[317] Section 38(5)(a) and 39(6)(a) of the Act. Also relevant is the degree of control a provider has in relation to the placement of advertisements on the service. We address this under 'Approach to control and working with intermediaries'.
[318] We set out our detailed approach to costs including the data used in Annex 8, 'Further detail on economic assumptions and analysis'.

information on the combined costs of our proposals in Volume 1, Section 6, 'Combined impact assessment'.

d) **Human rights impacts.** In assessing the proportionality of a proposed measure, we consider any potential impacts on human rights, in particular freedom of expression and privacy (including, to the extent relevant, data protection considerations). We set out our approach to considering human rights in paragraphs 5.61 to 5.95.

e) **Wider economic impacts and considerations.** We also consider wider impacts, such as impacts on advertisers and entities in the paid-for advertising supply chain, and on small and micro businesses.[319] Our consideration of wider economic impacts also relates to our duty to consider the desirability of promoting economic growth (the 'growth duty').[320]

f) **Equality and Welsh language impacts.** We have also assessed and have tried to mitigate where appropriate, equality impacts and Welsh language impacts.[321]

5.48 We note that these considerations are not exhaustive, and there are other factors we may consider on a measure-by-measure basis depending on the circumstances.

5.49 We set out the combined impacts of the proposed Codes in Volume 1, Section 6, 'Combined impact assessment' and detail specific impacts in the relevant measure sections across the consultation.

Who measures apply to

5.50 The fraudulent advertising duties apply to Category 1 and 2A services.[322] We have published Ofcom's 2026 register of categorised services ('the register'). We set out more information on regulated services in Volume 1, Section 2, 'Introduction' and Section 3, 'Online advertising ecosystem' and in Annex 2, 'Legal Framework'.

5.51 Our proposed package of measures applies to all Category 1 and 2A services on which UK users can encounter paid-for advertisements.[323]

5.52 The categorisation framework under the Act targets additional duties on services that meet certain threshold conditions, including conditions relating to their user numbers and functionalities.[324] In effect, the threshold conditions, as set out in secondary legislation, will cover the most widely used services.[325] Parliament designed the fraudulent advertising duties so that they apply to all Category 1 and 2A services. Further limiting our proposed

---

[319] As required under section 7 of the Communications Act 2003. See Volume 1, Section 6, 'Combined impact assessment' in paragraphs 6.21 to 6.22

[320] We set out information on the UK statutory Growth Duty (formally applied to Ofcom on May 21 2024) in the Volume 1, Section 2, 'Introduction' in paragraph 2.27 and Volume 1, Section 6, 'Combined impact assessment' in paragraphs 6.15 to 6.20.

[321] See Volume 1, Section 2, 'Introduction' in paragraphs 2.32 to 2.34 and Annex 6, 'Equality Impact Assessment and Welsh language assessment' for more information on our assessment of the equality and Welsh language impacts of our proposed measures.

[322] Thresholds are set out in the Online Safety Act 2023 (Category 1, Category 2A and Category 2B Threshold Conditions) Regulations 2025 [accessed 1 June 2026].

[323] For our proposed testing measure, there is a further scope requirement. The measure is applicable to providers of Category 1 and 2A services that make advertisement generation tools available to advertising account holders for paid-for advertisements placed on the service. See Volume 2, Section 5, under 'Scope of the proposed measure' for more information.

[324] Schedule 11 of the Act.

[325] See the Online Safety Act 2023 (Category 1, Category 2A and Category 2B Threshold Conditions) Regulations 2025; and the OSA Impact assessment, paragraph 80.

measures to sub-sets of Category 1 and 2A services would require clear evidence that an additional characteristic justified differential treatment in relation to what a particular measure involves and is designed to achieve.

5.53 We have considered whether narrowing the application of our proposed measures to a sub-set of services is warranted, taking into account both the impact (including cost) of individual measures and their likely combined effect. The evidence shows that fraud in paid-for advertising is likely to occur across the full range of Category 1 and 2A services that have paid-for advertising, and that each of our measures is likely to have important benefits for users of in-scope services. Our evidence also shows that perpetrators adapt their behaviour to evade detection. We are conscious of displacement effects and minimising risks that bad actors exploit differences in practice between Category 1 and 2A services with large user bases.

5.54 Taking into account the size of services in scope of fraudulent advertising duties, the risk of displacement, the nature and severity of harm posed by fraudulent advertising and our approach to situations where the provider lacks control over the placement of advertisements, we consider that it is appropriate and proportionate to apply our proposed measures to all Category 1 and 2A services on which UK users can encounter paid-for advertisements.

5.55 We will keep who our measures apply to under review as part of our iterative approach set out in paragraph 5.16.

Approach to user-to-user services and search services

5.56 In our Illegal Content Codes and Protection of Children Codes, there are some substantive differences between the measures recommended for user-to-user and search services. This is because user-to-user services and search services have different safety duties under the Act, and there are significant differences in how users encounter harmful content on these services.

5.57 In contrast, we are generally proposing the same measures for user-to-user and search services in our draft Fraudulent Advertising Codes. This is because:

a) The fraudulent advertising duties are closely aligned across service types.
b) Our evidence indicates that the core technologies driving the placement of paid-for advertising (auction systems, bidding tools, inventory management, targeting pipelines) operate in similar ways across both search and user-to-user services. This contrasts with the stark differences between technologies that enable user-generated content and those that generate search results. Further, where there are differences between services, these relate more to the advertising pathways used.[326]

5.58 We consider taking opportunities for alignment between the search and user-to-user Codes will provide benefits for coherence and useability of the Codes. This is particularly relevant as some user-to-user and search services may have paid-for advertisements placed from common or interconnected advertising systems.[327]

---

[326] We explain this further in Volume 1, Section 3, 'Online advertising ecosystem'.

[327] For example, Google Ads 'Performance Max campaigns' enables advertisers to access all of Google's channels, like YouTube and Search, see About Performance Max campaigns - Google Ads Help (accessed 17 June 2026). Microsoft's 'Performance Max ads' can similarly appear across Microsoft Advertising inventory (including search, display and other eligible Microsoft surfaces), see Microsoft Performance Max FAQs (accessed 17 June 2026).

5.59 We note that whilst our approach between search and user-to-user services is more aligned, we are still proposing to issue a separate Code for each. This makes it easier for providers of each kind of service to know which measures apply to them.

5.60 When describing a measure in relevant measure sections in Volumes 2 to 4, references to 'this measure' includes both the draft user-to-user measure and draft search measure. Where there are differences between them, we will explicitly note this.

Approach to human rights assessments

5.61 Our approach to assessing the impact of our proposed measures on human rights is the same as our approach set out in our Statement on Protecting People from Illegal Harms Online (December 2024 Illegal Harms Statement) and the Statement on Protecting Children from Harms Online (April 2025 Protection of Children Statement).[328] In this sub-section, we summarise that approach.

5.62 Part of our assessment of the impact of our measures on human rights is set out in this section (this is the case for cross-cutting points which apply across multiple proposed measures). Other parts of our assessment are set out in the sections explaining our individual measures (this is the case for points which apply specifically to individual measures). Therefore, our assessment for each measure is comprised of both this section and the discussion in the relevant measure specific section.

Rights relevant to our proposals

5.63 It is unlawful for Ofcom to act in a way that is incompatible with the European Convention on Human Rights (ECHR).[329]

5.64 Of particular relevance to Ofcom's functions under the Act are the right to freedom of expression (Article 10 ECHR) and the right to privacy (Article 8 ECHR). In formulating our proposals in this consultation, we have analysed where we have identified the potential for interference with ECHR rights to make sure any such interference is proportionate.

5.65 The right to freedom of expression includes the freedom to hold opinions and to receive and impart information and ideas without interference by public authority. Article 10(2) of the ECHR states that this right may be restricted in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

5.66 The right to freedom of expression does not solely apply to certain types of ideas or forms of expression,[330] and as such paid-for advertisements are protected by Article 10 of the ECHR, even where they promote commercial products and therefore comprise commercial expression.

5.67 Article 8(1) of the ECHR states that everyone has the right to respect for his private and family life, his home and his correspondence. Article 8(2) sets out limited qualifications,

[328] Ofcom, 2024. Introduction, our duties, and navigating the Statement, from paragraph 1.15; and Our Approach to developing Codes measures, from paragraph 1.97; Ofcom, 2025. Volume 4 What should services do to mitigate the risks of online harms to children, from paragraph 10.58 [accessed 13 June 2025]
[329] Section 6 of the Human Rights Act 1998.
[330] See, for example, *markt intern Verlag GmbH and Klaus Beermann v Germany* A/165 (1990) 12 EHRR 161

stating that public authorities must not interfere with the exercise of this right unless necessary in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

5.68 Other ECHR rights which may also be relevant to Ofcom's functions under the Act are the right to freedom of thought, conscience and religion (Article 9 ECHR) and the right to freedom of assembly and association (Article 11 ECHR). In addition, Article 1 Protocol 1 to the ECHR provides that natural and legal persons are entitled to the peaceful enjoyment of possessions and that they shall not be deprived of these except in the public interest and subject to the conditions provided for by law and general principles of international law. This may be relevant to the extent that any proposed measures mean that an advertiser loses marketable value in their business (on the basis of current trading practices rather than future profits).

Our approach to assessing rights impacts for fraudulent advertising

5.69 The rights outlined above are qualified rights. The need for any interference with these rights must be construed strictly and established convincingly. In particular, any interference must be:

a) prescribed by or in accordance with the law;
b) pursue a legitimate aim; and
c) be necessary in a democratic society, in other words, it must be proportionate to the legitimate aim pursued and correspond to a pressing social need.[331]

5.70 We recognise that in order for an interference with ECHR rights to be considered 'prescribed by law' it must have some basis in domestic law, and secondly, the relevant law should be accessible to the persons concerned, and formulated with sufficient precision to enable any individual to regulate their conduct. Additionally, any discretionary power must have sufficient safeguards to avoid the risk of arbitrary abuse of power.

5.71 In relation to fraudulent advertising, our starting point is to recognise that Parliament has determined, as set out in the Act, that providers of Category 1 and 2A services must use proportionate systems and processes designed to protect individuals from fraudulent advertising.[332] In practice, we consider this means taking proportionate steps to (a) prevent fraudulent advertising being shown to UK users on the service in the first place and (b) ensuring that where a provider becomes aware that fraudulent advert is being shown to UK users, taking steps to ensure this ceases swiftly. All of our proposed measures are designed to achieve one or both of these outcomes. Therefore, we start from the position that to the extent that our proposed measures involve an interference with ECHR rights this is prescribed by law.

5.72 The relevant legitimate aims that Ofcom acts in pursuit of in the context of our functions under the Act relating to fraudulent advertising include the prevention of crime and disorder, public safety and the protection of health or morals and the protection of the rights and freedoms of others. We note that protecting victims' and survivors' human rights is implicit in our duty to carry out our functions so as to secure the adequate protection of citizens from harm presented by content on regulated services.[333] As noted in our

[331] As set out in Articles 8(2), 9(2), 10(2) and 11(2).
[332] We set out the detail of the fraudulent advertising duties in Annex 2, 'Legal framework'.
[333] Section 3(2)(g) of the 2003 Act.

December 2024 Illegal Harms Statement, we do not consider it necessary to show that a particular harm to a user (such as harm from fraudulent advertising) infringes their human rights in order to show that the user should be protected from that harm.[334]

5.73 There is clear evidence which suggests that fraudulent advertising is widely prevalent and that it can have significant adverse impacts on individuals (as well as other businesses in the market) in the UK (see Volume 1, Section 4, 'Causes and impacts of fraudulent advertising', where we have set out this evidence). As such, we also start from the position that there is a pressing social need to (a) prevent fraudulent advertising being shown to UK users on the service in the first place and (b) ensure that where a provider becomes aware that fraudulent advert is being shown to UK users, it takes steps to ensure this ceases swiftly.

5.74 Our assessment of human rights focuses on whether a proposed measure that would be effective to achieve the legitimate aims may amount to a disproportionate interference with human rights. In order to assess this, we need to consider the impacts of each proposed measure on the rights that are being interfered with and specifically, whether the level of interference is no more than needed to secure the objective.[335] Where we have found a proposed measure is likely to interfere with these rights, we have explained why we consider this is proportionate to the Act's legitimate objectives (as outlined above), in which there is a pressing social need.

5.75 As noted in paragraphs 2.14 and 2.15 in Volume 4, Section 2, 'Advertising moderation', we will be consulting in autumn 2026 on a proposed proactive technology measure in relation to detecting fraudulent advertisements. We will assess the rights impacts arising from the proposed proactive technology measure at that time and have not considered them specifically here.

Freedom of expression (Article 10 of the ECHR)

5.76 In relation to the right to freedom of expression, as noted above, paid-for advertisements in most cases will consist of commercial expression. We note that freedom of commercial expression is generally treated as of less significance than other forms of speech, in particular freedom of political or artistic expression, which attract the highest levels of protection.[336] We have therefore taken this into account when assessing the proportionality of the proposed measures. We note that there may be impacts of particular significance in relation to political and public safety or other kinds of public interest advertising, which would attract a higher degree of protection than purely commercial expression. However, we consider that this is likely to represent only a small proportion of paid-for advertising overall, and may be less likely to be impacted by the measures than purely commercial advertising. Perpetrators of fraud will often be looking to make a financial gain and therefore will typically be advertising something for which they would take a payment, which will not generally be the case with political or public interest advertising (although we note that there may be other ways in which a fraudulent advertisement seeks to defraud users).

---

[334] December 2024 Statement, Our Approach to developing Codes measures, paragraph 1.99.

[335] We note that this is also a requirement under paragraph 10 of Schedule 4 to the Act. This requires measures to be designed in light of the principle of the importance of protecting the rights of users and interested persons to freedom of expression and privacy.

[336] See *R (on the application of British American Tobacco UK Ltd) and others v The Secretary of State for Health* [2004] EWHC 2493 (Admin), paragraph 28.

5.77 We note that it is open to a service provider to decide to remove paid-for advertisements or advertising accounts that are not linked to fraudulent advertisements. We cannot compel a provider to display advertisements that it does not wish to carry or allow accounts that it does not wish to permit, nor can we prevent a provider from removing advertisements or accounts that are not linked to fraud. We acknowledge the risk that, as a result of our recommendations, a provider may choose to take action against advertising or accounts that are not associated with fraudulent advertisements in order to ensure that it is compliant with its duties relating to fraudulent advertising. There may be some risk of providers choosing to err on the side of caution, resulting in 'over-moderation' or action on advertising which would not fall in scope of the definition of fraudulent advertisements under the Act. We are required by the Act to provide guidance to support service providers in understanding their regulatory obligations when making judgements about whether content is a fraudulent advertisement.[337] We consider that this will help providers understand the kinds of advertisements in relation to which they are required to act. Where possible, we have also sought to mitigate this risk. We have drawn out clearly in our Codes where we consider measures act as safeguards for human rights. However, the risk is ultimately one which arises from the scheme of the Act and cannot be mitigated entirely. We also note that, to some extent, this risk is mitigated by other incentives on service providers, such as those relating to maximising advertising revenue.

Privacy (Article 8 of the ECHR)

5.78 The right to respect for private life and correspondence is engaged where an individual has had a reasonable expectation of privacy. This is not simply limited to cases where a person can be said to have a reasonable expectation about the privacy of his home or personal communications; it extends to every occasion on which a person has a reasonable expectation that there will be no interference with the broader right of personal autonomy.[338] However, given the public nature of paid-for advertisements, we consider that in the majority of cases there will be minimal expectations of privacy in relation to the content of such advertisements and have taken this into account in our assessments.

Domestic laws relevant to the right to privacy

5.79 Along with the right to privacy conferred by Article 8 ECHR, there are various domestic laws relevant to this right. Service providers will need to ensure they comply with UK data protection law, which includes the Data Protection Act 2018, the UK General Data Protection Regulations (UK GDPR) and, where relevant, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR). Users' rights to data protection are regulated by the Information Commissioner's Office (ICO). The ICO has a range of data protection compliance guidance which we encourage service providers to consult. In particular, providers should familiarise themselves with the ICO Guidance on Online Safety and Data Protection[339] which includes its guidance on automated decision-making including profiling.[340]

---

[337] Section 193 of the Act, see Annex 9 to Annex 11.
[338] Per Lord Sumption in *R (on the application of Catt) (AP) v Commissioner of Police of the Metropolis* [2015] UKSC 9, paragraph 4.
[339] ICO, Online safety and data protection | ICO [accessed 10 June 2026]
[340] ICO, Automated decision-making, including profiling | ICO [accessed 10 June 2026] (in draft at the time of publication).

5.80 While Ofcom's remit is not to regulate data protection or provide guidance on compliance with data protection legislation, we will assess the impact of our measures against the main data protection principles where we consider these are also relevant to privacy. As part of our rights assessments, we have considered some important data protection principles, namely, lawfulness, fairness and transparency, data minimisation and accuracy.[341] We have also considered users' rights related to automated decision making. We have designed the proposed measures on the basis that those laws relevant to privacy rights will apply and that providers should be considering these data protection principles in their application of the measures, including through considering relevant guidance from the ICO. [342]

Freedom of thought, belief and religion and freedom of assembly and association (Article 9 and Article 11 of the ECHR)

5.81 In relation to rights under Articles 9 and 11 ECHR,[343] we consider that these rights will be engaged to a lesser extent in relation to paid-for advertising than user-generated content or search content more generally, given the predominantly commercial nature of the communications concerned. We therefore consider there will be minimal interference with these rights by our proposed measures and that, as such, any potential interference would be proportionate to the legitimate aims pursued by our proposed measures.

Advertisers' peaceful enjoyment of possessions (Article 1, Protocol 1 of the ECHR)

5.82 The right to peaceful enjoyment of possessions under Article 1 of Protocol 1 in no way impairs the right of the United Kingdom to enforce such laws as it deems necessary to control the use of property in accordance with the general interest. We consider the Act to be such a law, and we consider that the proposed measures are proportionate in relation to any interference with this right.

5.83 We recognise that any interference with the right to peaceful enjoyment of possessions will be greater where our proposed measures recommend restricting advertisers from accessing the advertising functionalities of a service or having their advertisements moderated. For example:

a) Moderating fraudulent advertising and banning advertising accounts which have posted it may lead to lost revenue where advertisements are no longer encounterable or able to be placed as a result, and this may affect revenue from both legitimate advertising and fraudulent advertising.
b) Measures concerning account checks and actions propose a set of onboarding checks which may, in some cases, prevent advertisers from accessing platforms.
c) Under the proposed measure on preventing fraudulent financial services advertising, advertisers who are unable to demonstrate that they are authorised, or otherwise legally permitted, to promote financial services and in line with a provider's financial services verification policy, may be prevented from advertising altogether. Even where advertisers are legally permitted to advertise in some contexts, providers may choose—within the flexibility afforded by the measure—to adopt more restrictive policies, such as limiting financial services advertising to FCA-authorised firms.
d) Under the proposed advertising intermediaries measure, where providers have insufficient control in relation to the placement of paid-for advertisements to apply

[341] Article 5(a), (c), and (d) of the UK GDPR
[342] See guidance from the ICO A guide to the data protection principles | ICO
[343] The right to freedom of thought, conscience and religion (Article 9) and the right to freedom of assembly and association (Article 11).

code measures (in whole or in part), they should use all reasonable endeavours to implement a version of the measure(s) not applied (or the relevant part of it) that is as similar to the measure as possible. 'All reasonable endeavours' should include requiring or working with advertising intermediaries involved in the placement of relevant paid-for advertisements to implement a version of the measure (or the relevant part of it) not applied. In practice, this may result in advertisers being required to meet additional verification or compliance requirements across the supply chain (and the resulting costs of this) or experiencing some variation in how measures are applied depending on the degree of control/intermediaries involved.

5.84 Taken together, these measures may impose additional requirements or constraints on advertisers and may, in some cases, affect the commercial value derived from advertising activity. However, the impacts are likely to largely fall on bad actors and high-risk accounts. Further, in relation to some of the measures referred to above, interference is likely to stem from providers choosing to prohibit broader categories of advertisement than is a requirement to implement these measures and is more than is required by the Act. This would be a matter of their own choice. More generally, we have also taken into account the context in which paid-for advertisements will be displayed to users on Category 1 and 2A services. In particular, we note that given the commercial incentives on both providers and advertisers, both such parties are incentivised to maximise revenue which may also influence the approaches taken when implementing our proposed measures and in turn may affect the level of interference with human rights. Overall we consider the measures are justified and proportionate in light of the significant harms associated with fraudulent advertising, particularly in high-risk sectors.

Service Providers' peaceful enjoyment of possessions (Article 1, Protocol 1)

5.85 We also recognise that some of the proposed measures may engage the Article 1 Protocol 1 rights of service providers.

5.86 The implementation of some of the proposed measures is likely to involve providers incurring both one-off and ongoing costs which could in some cases reduce their profitability and led them to losing marketable value in their business. Some proposed measures may also affect the way in which providers are able to monetise their services, particularly in relation to higher-risk advertisers, and reduce advertising volumes. We have discussed these costs and impact in relation to each proposed measure and in the combined impact assessment. These include the development and operation of systems for account checks and financial services verification, as well as the governance processes needed to support and review these systems over time. While such costs are a common feature of regulatory compliance, they may represent an interference with providers' economic interests, in that they may reduce profitability or require the reallocation of resources.

5.87 However, we consider that any such interference with providers' economic interests is justified and proportionate. The measures pursue a clear and important public interest objective, namely the protection of users from fraudulent advertising, which is associated with significant financial harm. The approach we propose allows a degree of flexibility, enabling providers to design systems that meet the required outcomes in a way that aligns with their business models. In many cases, the measures build on practices that are already in place across the industry, meaning that the incremental burden is reduced.

5.88 In addition, providers retain a degree of commercial autonomy within the framework of the Codes. They are not required to adopt a single prescribed model, nor are they prevented from making their own choices about how to balance compliance with other business objectives, provided that they meet the relevant duties. Taking these factors together, we consider that the impact on providers' Article 1 Protocol 1 rights is proportionate to the legitimate aim pursued.

Intermediaries' peaceful enjoyment of possessions (Article 1, Protocol 1)

5.89 We further recognise that the proposed advertising intermediaries measure may have implications for intermediaries in the advertising supply chain. This proposed measure may lead to intermediaries being asked to implement, support, or facilitate certain measures. This may in turn give rise to additional compliance costs, changes to technical systems, or adjustments to contractual arrangements with clients and partners. There may also be indirect commercial effects, for example where the exclusion of high-risk advertising reduces revenue flowing through certain parts of the supply chain.

5.90 Intermediaries are not themselves subject to duties under the Codes, and providers retain flexibility as to how they engage with them in order to meet their obligations. The purpose of the advertising intermediaries measure is to ensure that the effectiveness of the regulatory framework is not undermined by differences in control across advertising pathways.

5.91 In this context, any interference with the Article 1 Protocol 1 rights of intermediaries is limited and proportionate.

Positive effects of the proposed measures on human rights

5.92 We recognise that online safety regulation may also help protect individuals' human rights. There is evidence[344] that the presence of fraud may undermine the trust people have in institutions and in the form of communication that enabled the fraud, as well as having effects on the market and legitimate businesses. This may lead to individuals being less willing to use a service to express themselves and may impact on the ability of providers and advertisers to generate engagement and revenue on the service. As such, where our proposed measures help to reduce the presence of fraudulent advertising on a service, this may help individuals to feel safer and more able to use a service and therefore more able to exercise their rights to freedom of expression. This in turn could positively impact providers' and advertisers' rights as protected by Article 1 Protocol 1. Addressing fraudulent advertising could also help to protect users' Article 1 Protocol 1 rights by reducing the risk that they are deprived of their property (e.g. money, assets or economic interests) through fraud.

5.93 We note our proposed measures could also have a positive effect on individuals' right to privacy as some paid-for advertisements may misuse personal data or likenesses. The proposed measures could therefore assist in preserving individuals' rights to privacy, where they lead to the reduction in the presence of fraudulent advertisements which misuse personal data or likenesses on services (either directly through action on the advertisement itself or the associated advertising account, or indirectly through changes to overall systems and processes). There may also be positive effects to privacy rights where the proposed measures lead to improved awareness of and adherence to relevant data protection

[344] See paragraph 1.63 of Volume 1, Section 4, 'Causes and impacts of fraudulent advertising'.

legislation and guidance. Where our measures encourage better management practices, this may also lead to a provider being more likely to comply with its obligations under privacy and data protection laws (as well as, for that matter, other laws such as those relating to consumer protection and equality). As such, our proposed measures may help to safeguard these. We have not reiterated these benefits in the rights assessments set out in relation to each proposed measure as they are cross-cutting. However, many of the measures proposed will attract these benefits and we have taken this into account in considering the proportionality and necessity of any interference by the measures with human rights.

Overall provisional conclusion

5.94 Our provisional conclusion is that there is no less intrusive way of achieving the same aims with comparable effectiveness, and we have included safeguards in our proposed measures to ensure relevant rights are protected. We have clearly indicated in the Fraudulent Advertising Codes where we consider proposed measures act as safeguards for a relevant right.[345]

5.95 Overall, we have sought to strike a fair balance between securing the legitimate aims set out in the Act in relation to fraudulent advertising (and their human rights in respect of this) and the ECHR rights of users, advertisers, other interested persons (including for example, persons who host websites that appear in search results or who may be featured in content on regulated services or whose content might be on those services regardless of whether or not they are service users), and service providers, as relevant.

[345] We note that it is a requirement under paragraph 10 of Schedule 4 to the Act which requires measures to be designed in light of the principles of the importance of protecting the rights of users and interested persons to freedom of expression and privacy, and (where appropriate) to incorporate safeguards for the protection of those principles.

6. Combined Impact Assessment

What is this section about?

We have assessed the individual impact of each of the proposed measures in Volumes 2 to 4. As set out there, we consider each of the proposed measures to be effective and significantly beneficial in their own right.

Here we have considered the cumulative impact of our proposals. We consider that this proposed package of measures would be effective in combatting fraudulent advertising. Collectively, we consider the proposed package would have even more significant benefits as the proposed measures are mutually reinforcing, interlocking and not duplicative.

Though the costs of the proposed measures could be significant for some providers, we consider it to be proportionate to the scale of harm fraudulent advertising causes. On balance, our provisional view is that the package of proposed measures set out in this consultation would be proportionate. This conclusion is further supported by the fact that there are a number of factors which would likely mean that in practice the costs of the proposed measures would likely tend to be lower than the headline estimates set out in this document.

Consultation question

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

Introduction

6.1 In this consultation, we are proposing a package of measures designed to tackle fraudulent advertising.

6.2 In Volumes 2 to 4 we describe and assess the impact of each of the proposed measures individually.

6.3 As set out below, the proposed measures are designed to be mutually reinforcing, interlocking, and not duplicative. In addition to assessing the impacts of the measures individually, it is therefore important to consider the combined impact of the package we are proposing, which we do in this section.

Context

6.4 Fraud is the most common crime in the UK,[346] and the resulting economic and social costs to individuals are substantial.[347] Advertising is the second most common content type used

[346] National Economic Crime Centre, 2025. National Economic Crime Centre Annual Report. [accessed 25 March 2026]; UK Finance, 2025. Annual Fraud Report 2025. [accessed 5 February 2026].
[347] The Home Office estimated the economic and social cost of fraud against individuals to be £9.2 billion in the year ending March 2024. Source: Home Office, 2026. Economic and social cost of fraud 2023 to 2024. [accessed 21 April 2026];

by fraudsters to reach users online,[348] and bad actors are likely increasingly using paid for adverts to reach users at scale.[349] Our own estimates suggest that the costs of fraudulent advertising to UK users and the wider UK economy could exceed £800 million per year.[350]

6.5 Victims of fraudulent advertising face a range of impacts including: financial loss,[351] emotional distress, erosion of trust and multifaceted impacts on their lives. There are also wider impacts, including distortions to markets, reduced trust in legitimate (often smaller) businesses, and the funding of criminal activity, all of which can cause significant harm to individuals.[352]

6.6 We are proposing a layered approach to tackling fraudulent advertising, by proposing measures designed to:

i) Stop fraudsters posting fraudulent advertisements in the first place;
ii) Improve the speed at which fraudulent advertisements are detected; and
iii) Ensure swift action, once detected, to remove fraudulent advertisements.[353]

Benefits

6.7 As we explain in Volumes 2 to 4, our analysis indicates that each of the measures we are proposing will be effective and significantly beneficial in their own right.

6.8 Collectively, we consider the proposed package of measures to have even more significant benefits, as the proposed measures are mutually reinforcing, interlocking and not duplicative. For example:

a) The fraud indicator assessment would yield insights on how fraudulent advertising manifests on a platform and the material risks associated with content and advertising accounts.[354] These insights can then be fed into other mitigations (for example, prioritisation of advertising moderation, training and materials and account checks),[355] to apply them in a more effective and proportionate manner.
b) Our proposed suite of Governance measures should mean greater oversight and accountability to support implementation of all the other proposed measures.[356]

---

[348] We note that Ofcom research indicates that c.20% of victims of online fraud are reached via online advertisements (search result or listing 9%; an advertisement integrated in social media 8% and; an advertisement before a video played 3%). Source: Ofcom, 2023. Executive Summary Report: Online Scams & Fraud Research.

[349] Sparkninety, 2022. Online Advertising Programme Market Insights. [accessed 13 March 2026]; Center for Countering Digital Hate, 2026. Scambook: How Meta helps Medicare scammers target seniors. [accessed 15 May 2026]; Juniper Research and Revolut, 2026. Protecting Users from Scam Ads. [accessed 13 February 2026].

[350] We provide more detail on how we calculated this estimate in Annex 8, 'Further detail on economic assumptions and analysis'.

[351] As noted in Volume 1, Section 4, 'Causes and impacts of fraudulent advertising', sub-section 'Impact of fraudulent advertising', financial losses can vary from relatively small to life changing sums. It is further worth noting that even the loss of small sums of money can have hugely detrimental impacts on vulnerable users.

[352] See Volume 1, Section 4, 'Causes and impacts of fraudulent advertising', sub-section 'Wider impacts'.

[353] For more information on our layered approach see Volume 1, Section 5, 'Approach to codes', sub-section 'Approach to designing our fraudulent advertising proposals'.

[354] For more information on this proposal see Volume 2, Section 3, 'Fraud indicator assessment'.

[355] For more information on these proposals see Volume 4, Section 2, 'Advertising moderation' and Volume 3, Section 2, 'Account checks and actions'.

[356] For more information on these proposals see Volume 2, Section 4, 'Governance and accountability'.

c) Our layered approach helps to ensure we are tackling the harm both at an upstream and downstream layer, and the mitigations are reinforcing.[357] For example:

i) More effective account verification and bans would mean less fraudulent advertising should need to be tackled via moderation or reports;[358]
ii) Better reporting, enhanced by a Direct Reporting Channel (DRC) and an effective advertising library,[359] should lead to more effective moderation of content; and
iii) Enhanced testing of AI tools should mean fewer vulnerabilities that could be exploited by fraudsters,[360] and should mean fewer content reports and less moderation activity.

6.9 We consider that this proposed package of measures would be effective in combatting fraudulent advertising. As such, we think the aggregate benefits the package would deliver to be very significant.

6.10 It is not possible to quantify with precision the total benefits, given the complexities of calculating how much fraudulent advertising would be prevented by the proposed package of measures. However, given the scale of harm caused by fraudulent advertising, even if the proposed package of measures only resulted in a relatively small reduction in fraudulent advertising, the benefits could be in the billions of pounds over a 10-year period.

6.11 For example, if implementing our proposed measures resulted in a reduction in exposure to fraudulent advertising of between 10% and 30%, this could mean a reduction in costs to UK users and the wider economy of £70 to £240m per year, which equates to benefits of between £600m to £2bn over a ten-year period in today's money. We note this range of estimates likely understates the magnitude of the benefits as it does not capture the full range of expected benefits. For example, the benefits from increased user trust in legitimate advertising which can lead to increased demand, or the benefits of diverting the resources currently going to organised crime to more productive uses, or the benefits of discouraging future harm that would follow from implementation of the proposed package.

Table 6.1: Provider estimates of UK ad volumes and prevalence of fraudulent advertising (FA)

Service	UK ad volume[361]	Prevalence of FA[362] (estimates from services vary from close to zero to c.2% share of ad impressions)
Meta	[✂]	[✂] [✂]
Google	[✂]	[✂]

[357] For more information on our layered approach see Volume 1, Section 5, 'Approach to codes', sub-section 'Approach to designing our fraudulent advertising proposals'.
[358] For more information on our proposals relating to accounts see Volume 3, 'Ensuring account integrity'.
[359] For more information on these proposals, see Volume 4, 'Moderation'.
[360] For more information on this proposal, see Volume 2, Section 5, 'Testing advertisement generation tools'.
[361] UK ad volume strictly relates to the number of paid for advertisements shown on the service. It does not indicate which services host the largest number of fraudulent advertisements. Source: [✂].
[362] "Impressions" refers to the number of times an advertisement is shown to users, with each instance in which a user sees an advertisement, or an advertisement is placed, counted as one impression. The share of impressions attributable to fraudulent advertising does not necessarily correspond to the share of advertisements that are fraudulent, as fraudulent and non-fraudulent advertisements may generate different average numbers of impressions. Source: [✂].

Service	UK ad volume[361]	Prevalence of FA[362] (estimates from services vary from close to zero to c.2% share of ad impressions)
Microsoft	[✂]	[✂]
Amazon	[✂]	[✂]
TikTok	[✂]	[✂]
X	[✂]	[✂]
Snapchat	[✂]	[✂]
Pinterest	[✂]	[✂]
LinkedIn	[✂]	[✂]

Costs on service providers

6.12 In Volumes 2 to 4 we assess the costs to providers of each of the proposed measures and present our estimates of the costs we expect service providers would incur to implement the proposed measures.[363]

6.13 As a package, the total costs to providers could be substantial. Our estimates suggest that this could cost in the low tens of millions of pounds for some categorised services. Specifically, for the proposed measures where we have been able to quantity costs, total Year 1 costs could range from over £500K to around £4 million, with total ongoing costs ranging from £2 million to over £5.5 million. On a 10-year net present value (NPV) basis, this equates to estimated costs of £15 million to £45 million per service.

6.14 However, it is important to contextualise these costs:

- Many of the proposed measures in the package offer significant flexibility to providers (for example, the fraud indicator assessment, or most of the measures adapted from our Illegal content Codes of Practice[364]). The inherent flexibility is well suited to the adversarial nature of fraudulent advertising harm, and enables easier adaptation to new fraudster tactics. It also allows providers the option to adopt an approach that works best for their business model, and to leverage existing infrastructure and expertise.
- Though we have impact assessed each of the proposed measures separately, we expect there to be cost synergies across the package. Several proposals rely on overlapping systems, processes and data, which we have not been able to account for in our cost estimates. Action taken to implement one measure may support the implementation of others.
- Most in scope services generate significant revenues from online advertising, and it is a very profitable activity for many of them. Moreover, we consider that loss of revenues

[363] We detail our approach to estimating costs including the sources of evidence used in Annex 8, 'Further detail on economic assumptions and analysis'.
[364] For more information on these adapted measures, see Volume 1, Section 5, 'Approach to codes', sub-section 'Approach to regulatory alignment'.

associated with fraudulent advertisements are not a relevant consideration for our assessment.

- Our proposed measures apply to Category 1 and Category 2A services. These are the largest services, and so we would expect them to be fairly well resourced.
- Some providers will already have similar measures in place to tackle fraudulent advertising. This means that the likely incremental costs associated with these proposed measures will be more modest than the estimates above suggest.

Other relevant considerations

Economic growth

6.15 Ofcom is required, when exercising our regulatory functions, to have regard to the desirability of promoting economic growth, including through considering the importance of ensuring the regulatory action we take is necessary and proportionate.[365] This duty is referred to as the "growth duty". The growth duty has applied to our online safety functions since 6 April 2026, following the end of a time-limited exclusion for these functions.

6.16 We are also required to have regard to the Government's statutory guidance on the growth duty.[366] That guidance explains that the duty needs to be considered alongside our other statutory duties, and that its purpose is not to achieve or pursue economic growth at the expense of necessary protections.[367] Among other things, it also identifies particular drivers of economic growth, including innovation, investment and competition.

6.17 In line with the statutory guidance, we have considered the impact of these measures on key drivers of economic growth, including innovation, investment and competition. We anticipate that any impact on UK economic growth resulting from the proposed measures will be limited. For the majority of service providers, the direct costs associated with implementation are expected to broadly reflect the scale of advertising activity and the corresponding risk profile of each service. Consequently, the more significant costs are likely to be incurred by platforms with substantial advertising revenues, which are well placed to accommodate these requirements. As the proposed Codes apply solely to categorised services, we expect these businesses to be able to implement the recommended measures without any material effect on their capacity to invest, innovate, or compete effectively within their respective markets.

6.18 Where possible, the measures take a technology-neutral approach and are not intended to mandate the use of specific technologies, system architectures, or model types. Service providers may achieve the required outcomes through alternative measures, allowing them the flexibility to implement the recommended measures in a proportionate way that minimises unnecessary burden.[368]

---

[365] Section 108 of the Deregulation Act 2015.
[366] Section 110(3) of the Deregulation Act 2015.
[367] Department for Business and Trade, 2024. Growth Duty: Statutory Guidance – Refresh. [accessed 18 June 2026].
[368] Service providers do not need to follow the Codes and may seek to comply with their safety duties by taking what the Act calls "alternative measures". Where providers take alternative measures, they must be able to show how those measures ensure they are operating their services in compliance with the fraudulent advertising duties set out in sections 38 and 39 of the Act.

6.19 We consider it unlikely that the proposed measures will give rise to significant indirect effects on adjacent markets or the wider economy. The proposed measures are targeted specifically at the prevention, detection, and mitigation of fraudulent advertising. We have sought to mitigate identifiable potential impacts, for example frictions for advertisers, such as losing access to the service if they are falsely suspected to have posted fraudulent advertising, by recommending an appeals mechanism. As a result, we consider the proposed measures unlikely to generate material spillover effects or indirect costs beyond the services and advertising activities directly in scope.

6.20 In addition, the package may generate modest supply-side benefits by supporting a more trusted and predictable online advertising environment. By reducing the prevalence of fraudulent advertising and improving confidence in online advertising systems, the proposed measures may strengthen conditions for legitimate advertisers, support user trust, and contribute to a healthier digital advertising ecosystem. While these effects could support economic activity within the online advertising market, we expect any positive impacts on aggregate economic growth to remain modest.

Small and micro businesses

6.21 When considering the proportionality of our measures we have considered the potential impacts on small and micro businesses.[369] We have done this because we have a specific duty to consider them.[370]

6.22 We note that none of the providers of Category 1 or 2A services in scope of the fraudulent advertising duties are small or micro businesses. As such, the proposed measures do not impose direct costs on small or micro businesses. We have however considered impacts of our proposed measures on other small and micro businesses (e.g. small advertising agents or businesses) that may face indirect costs (including in Volume 1, Section 5, 'Approach to codes' under the sub-heading 'Advertisers' peaceful enjoyment of possessions (Article 1, Protocol 1 of the ECHR'). These businesses might be impacted by some of our proposed measures, for example by going through account checks and verification processes and having their advertisements moderated.[371] We consider those impacts to be proportionate in light of the benefits provided by those proposed measures.

Provisional conclusion

6.23 The analysis in this consultation suggests that the proposed measures in question would be costly but proportionate to the scale of the harm fraudulent advertising causes. On balance,

[369] We define such businesses based on the number of full-time equivalent employees, which we understand to be commonly used parameters for defining these businesses across UK Government departments. We define small businesses as those that employ between 10 and 49 full-time equivalent employees, and micro businesses as those that employ between one and nine full-time equivalent employees. We appreciate that not all Government bodies use exactly the same definitions. For example, some also refer to revenue and assets. The definition we propose is consistent with that used by the Regulatory Policy Committee. It would not make a material difference to our impact assessment if another common definition of small and micro business (such as that consistent with the Companies Act 2006) were used instead. Source: Regulatory Policy Committee, 2019. Small and Micro Business Assessments: guidance for departments, with case history examples, August 2019. [accessed 26 June 2026].

[370] See section 7(4A) of the 2003 Act.

[371] See Volume 3, Section 2, 'Account checks and actions' and Volume 4, Section 2, 'Advertising moderation' for more information on these proposals.

our provisional view is that the package of proposed measures set out in this consultation would be proportionate.

6.24 This view is reinforced by the fact that many of the proposed measures offer significant flexibility, that there are likely cost synergies across the package, and in many cases the costs of the proposed measures are very small compared to the revenues providers generate from online advertising. We note that Category 1 and Category 2A services are some of the largest services, and so we would expect them to be fairly well resourced. We also consider our estimates underplay the likely benefits of the proposed package. As noted in paragraphs 6.10 and 6.11, not all benefits can be quantified, and we have not been able to incorporate several potential benefits associated with implementation of our proposed package of measures. In undertaking our assessment, we have looked at benefits in light of the current situation, where providers have already implemented some mitigations.[372] This could also understate the likely overall benefits of the package.

[372] Our counterfactual for costs is often undertaking the mitigation from scratch. In looking at the benefits, we have looked at the current situation, where there is often partial implementation of the measure.