Walpole

Consultation coversheet
Fraudulent Advertising Codes Consultation
Deadline: 2 October 2026

Basic details

Consultation title: Fraudulent Advertising Codes Consultation
To (Ofcom contact): FraudulentAdvertisingConsultation@ofcom.org.uk
Name of respondent: [redacted]
Representing (self or organisation/s): Walpole
Address (if not received by email):

Confidentiality

Please tick below what part of your response you consider is confidential, giving your reasons why
> Nothing ☐
> Name/contact details/job title ☐
> Whole response ☐
> Organisation ☐
> Part of the response ☐
If you selected 'Part of the response', please specify which parts:

Walpole

Fraudulent Advertising Codes Consultation
Deadline: 2 October 2026

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.

These services, known as categorised services, are some of the most widely-used online services in the UK.

The draft includes Ofcom's 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 or non-sponsored search content.

Walpole's Response

Walpole is the sector body for the British luxury industry, worth £81bn to the UK economy and supporting 454,000 jobs. With a mission to promote, protect and develop British luxury, Walpole gives a voice to over 250 members and is recognised in both Westminster and Brussels. It is a convener for the sector and commissions industry research. Walpole also develops the industry and supports future growth through its Brands of Tomorrow incubator programme, leading trade missions to drive growth overseas and positioning brands for long-term success through its sustainability community.

Volume 1: Context

Online advertising ecosystem

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

Major advertising platforms are structurally exposed to fraudulent and illegal advertising and may derive substantial revenue from it unless they **implement sufficiently robust controls**. Therefore, it is crucial that the Code impose clear **preventive obligations**.
We support a framework that places meaningful responsibility on the platforms that design, sell, target and monetise advertising inventory.
In practice, this requires:

1. stronger, clearer Know your Business Customer (KYBC) requirements for advertisers;
2. explicit "stay-down" expectations to prevent fraudulent advertisers and advertisements from repeatedly reappearing;
3. more robust, proactive risk-assessment and mitigation obligations; and
4. clearer consequences when platforms fail to use best efforts to prevent foreseeable, repeated harm.

A framework that relies too heavily on post-publication notice and takedown will be insufficient. Fraudulent advertising is often fast-moving, cross-border and highly adaptive. Effective protection requires **upstream controls** before advertisements are served, alongside reactive removal once harmful content appears.

Luxury brands are particularly exposed to fraudulent advertising, counterfeiting and brand impersonation due to the strength of their intellectual property, global brand recognition and the significant price differential between genuine and counterfeit goods.

Our members' experience demonstrates that fraudulent advertising should not be viewed in isolation. It forms part of a wider online ecosystem spanning paid advertising, social media content, influencers, user accounts, online marketplaces, search engines, messaging services and standalone websites. **Platforms should therefore consider the full consumer journey**, including coordinated activity across accounts and services that directs consumers towards fraudulent offers.

We broadly support Ofcom's proposed measures and agree that fraudulent advertising harms both legitimate businesses and consumer trust. **Robust account integrity and advertiser verification requirements** are particularly important to ensure advertisers genuinely represent the brands and organisations they claim to act for.

However, the luxury sector's experience also highlights the limitations of drawing too narrow a distinction between paid advertising and other forms of online commercial promotion.

While user-generated content is outside the scope of this consultation, **influencer content often performs the same commercial function as advertising by promoting products**, shaping purchasing decisions and directing consumers to retailers, marketplaces and third-party websites, fitting within Advertising Standards Authority's (ASA) definition of influencer advertising.[1] Research by ASA[2] has found that consumers do not always clearly recognise influencer marketing, reinforcing the blurred distinction between advertising and organic content.

This is especially relevant in the **context of counterfeit goods**. Bad actors increasingly replicate legitimate influencer marketing techniques to create a perception of authenticity, build consumer trust and drive consumers towards infringing products.

Our sector has also witnessed the **growing role of influencers and social media personalities in normalising counterfeit goods**. Counterfeit products are frequently presented as attractive, low-cost alternatives to genuine items, particularly to younger consumers.

[1] https://www.asa.org.uk/advice-online/recognising-ads-social-media.html

[2] https://www.asa.org.uk/resource/consumer-awareness-and-understanding-of-influencer-marketing.html

Luxury brands can provide significant evidence regarding **repeat infringers**, brand impersonation, trademark misuse, links between social media promotion and marketplace listings, and the rapid migration of fraudulent actors between accounts following enforcement action.

We encourage Ofcom to expand its approach **beyond paid-for advertising and consider the role of influencer-generated promotional content** within the wider online advertising ecosystem. **Greater cooperation and structured information-sharing between platforms, regulators, rights holders and enforcement authorities** will also be essential to identifying repeat infringers, disrupting coordinated fraudulent activity and preventing bad actors from re-emerging across multiple services.

Looking ahead, these **risks are likely to intensify as AI-enabled commerce and agentic AI become more widespread.** As AI systems increasingly discover, compare, recommend and potentially purchase products on consumers' behalf, fraudulent advertisements, impersonation websites and counterfeit listings could influence not only consumer decisions but also the automated systems that support them, amplifying the speed and scale of harm.

Strong advertiser verification, proactive detection measures, provenance signals, rapid removal of fraudulent content and platform regulatory liability will therefore be essential to ensuring that both consumers and AI-powered systems can distinguish legitimate businesses from fraudulent actors.

Causes and impacts of fraudulent advertising

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

We broadly agree with Ofcom's assessment and welcome its recognition that fraudulent advertising is an evolving harm that exploits trusted brands, new technologies and online commercial ecosystems, causing damage to consumers, legitimate businesses and the wider economy.

However, greater emphasis should be placed on the **close relationship between fraudulent advertising, intellectual property infringement and counterfeiting.** Luxury brands are particularly vulnerable because fraudsters frequently misuse trademarks, brand imagery and established reputations to promote counterfeit goods, impersonate legitimate businesses and deceive consumers. The resulting harm extends well beyond financial loss, undermining brand integrity, eroding consumer confidence and imposing significant enforcement costs on rights holders.

Advertising platforms can play a central role in the promotion, amplification and **monetisation of illegal commercial activity online**.[3] This includes counterfeit goods and other illicit trade; the growing normalisation and promotion of "dupes", which can blur the distinction between lawful competition and unlawful imitation; brand and individual impersonation; online fraud and scams; and fake promotions or deceptive offers that use paid placement to create an appearance of legitimacy.

This is not simply a hosting issue. Platforms onboard advertisers, process payments, provide targeting tools, optimise delivery and profit from engagement and conversion. That active role justifies stronger accountability where reasonable and proportionate safeguards are not in place.

We believe the Code should contain stronger and more explicit KYBC expectations. Platforms should be required to apply meaningful KYBC controls before allowing advertisers to place paid-for ads.

At a minimum, KYBC should include, where relevant:

1. verification of the advertiser's legal identity and business registration;
2. verification of contact details and country of establishment;
3. verification of payment method consistency with the declared business;
4. periodic re-verification, not only one-off onboarding checks;
5. enhanced scrutiny for newly created accounts, high-velocity campaigns, recently registered domains, and repeat policy evaders.

Fraudulent advertising creates significant **risks for consumers**, including financial loss, identity theft, deception as to the origin or authenticity of goods, exposure to unsafe or non-compliant products and scams that exploit trust in well-known brands or public figures.

It also distorts competition by allowing bad actors to purchase visibility through counterfeit offers, impersonation and deceptive claims, placing legitimate businesses that invest in quality, safety, compliance and reputation at a disadvantage. Repeated exposure to such content can further weaken trust in legitimate brands, dilute brand equity and normalise unlawful commercial practices.

We encourage Ofcom to view **fraudulent advertising as part of a wider consumer journey** rather than as an isolated piece of paid-for content. Consumers may move between influencer content, paid advertisements, online marketplaces and external websites before making a purchase, while fraudsters increasingly exploit the blurred boundaries between advertising, organic content and online commerce. Although user-generated content falls outside the scope of these Codes, influencer promotion of counterfeit goods and other

[3] Public reporting has underlined the scale of the problem. Reuters reported on internal Meta documents suggesting that the company had internally estimated that up to 10% of its 2024 revenue – or $16 billion - was linked to ads associated with scams, illegal or prohibited products and other high-risk advertising activity.

deceptive practices forms part of the wider risk landscape and should be considered in future regulatory work.

Greater emphasis should also be placed on repeat and coordinated offending. Fraudulent actors frequently recreate accounts, move between platforms, establish linked networks and use multiple identities to evade enforcement. This underlines the need for robust platform-level accountability, stronger cross-platform cooperation and more effective mechanisms for identifying repeat offenders.

Any verification measures must be supported by effective action against repeat offenders. Removing a single advertisement is insufficient if the same actor can immediately return through a new account, domain, payment instrument or affiliated business identity. The Code should therefore establish **a clear "stay-down" expectation**.

To meet this expectation, platforms should be required, on a best-efforts basis, to take reasonable technical and organizational measures to prevent the reappearance of:

1. advertisers previously identified as fraudulent;
2. identical or materially similar fraudulent advertisements;
3. linked accounts or networks associated with previous fraud; and
4. repeated brand-impersonation campaigns and counterfeit offers.

If a platform fails to use best efforts to implement such measures, and fraudulent activity repeatedly reappears despite being reasonably foreseeable and technically addressable, that failure should be taken into account when assessing the platform's compliance and liability.

The Code should also address more explicitly the **risks posed by brand impersonation**, **individual impersonation and counterfeit advertising**. These forms of fraud are particularly harmful because paid placement can create a false impression of legitimacy. Consumers may reasonably assume that sponsored content featuring a recognised brand name, logo, executive identity, celebrity image or product visual has been subject to meaningful checks and verification.

We therefore recommend prioritised reporting channels for verified rights holders and affected businesses; accelerated review and takedown processes where credible evidence is provided; stronger measures against repeat counterfeit advertisers and impersonation networks; and greater use of technical tools to identify duplicate creatives, repeated claims, linked domains and associated accounts.

Finally, we welcome Ofcom's recognition that **AI** is reducing the cost and increasing the scale of fraudulent advertising. Looking ahead, these challenges are likely to intensify as AI-generated content becomes more sophisticated and AI assistants and agentic systems become increasingly embedded in online commerce. It will therefore be important to ensure that the regulatory framework remains capable of addressing both AI-enabled fraud and

the growing role of AI in how consumers discover, evaluate and purchase products and services.

Where a platform fails to use best efforts to implement meaningful KYBC controls and take-down and stay-down requirements, to put in place proportionate and effective measures to identify its advertisers, and to prevent illegal content from appearing or reappearing, and where that failure contributes to foreseeable harm, the platform should be held accountable under the regulatory framework.

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

We agree with the characteristics identified, namely the risks associated with brand and public-figure impersonation, cloaked landing pages, unusual URLs, generative AI/deepfakes and suspicious account behaviour. We would additionally encourage Ofcom to pay particular attention to unauthorised use of legitimate trademarks and brand imagery, substantial or implausible discounts, repeated or coordinated accounts, rapid account creation following enforcement action, and links directing consumers to counterfeit marketplaces or imitation websites.

Ofcom rightfully identifies practices such as "phoenixing", "lifeboating", and affiliate networks that allow fraudsters to re-establish or scale activity. As AI uses become more sophisticated, this further strengthens the case for proactive platform monitoring and accountability.

4. **Do you agree with our proposed approach to the Codes? Please provide any arguments and supporting evidence.**

We broadly agree with Ofcom's proposed approach, particularly the layered model combining prevention, account-level controls, moderation, reporting and swift removal. We also support the emphasis on safety by design, governance and platform accountability, rather than relying primarily on consumers or rights holders to identify fraud after harm has occurred.

We particularly welcome the recognition that current practices are not going far enough, and that regulatory intervention and enforcement is required at this stage to drive forward better standards. We also strongly welcome Ofcom's approach to regulatory alignment, including its consideration of relevant requirements under the EU Digital Services Act. This alignment is not only appropriate for our sector but helps reduce unnecessary fragmentation and strengthen cross-border identification of fraudulent advertising and make it more difficult for bad actors to exploit regulatory differences between jurisdictions.

However, we encourage Ofcom to maintain a genuinely iterative approach. Fraudulent advertising evolves quickly, particularly as emerging technologies such as AI enable more sophisticated impersonation, automation, and scaling of fraudulent activity. We note that

these codes have been described as an initial, first iteration which will be a foundation to build on over time. In future iterations we strongly recommend consideration and integration of the wider ecosystem surrounding paid advertising, including influencers, individual actors and other forms of commercial content that can direct consumers towards counterfeit or fraudulent offers.

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

Yes, we consider the overall burden on in-scope service providers to be proportionate to the scale and seriousness of the harm caused by fraudulent advertising. While we understand that Ofcom estimates that implementation could involve significant costs for some services, these costs should be considered in the context of the substantial advertising revenues generated by the services concerned and the significant economic and consumer harms the measures are intended to address.

We also agree that the measures should reinforce one another and create efficiencies across the system. Stronger account verification and effective advertiser bans should reduce pressure on downstream moderation and reporting, while improved reporting mechanisms and advertising libraries should support earlier and more accurate detection.

While we appreciate the compliance costs involved, from the perspective of our members as businesses and rights holders affected by fraudulent advertising, the compliance burden on platforms should be seen within the wider context and costs being borne by legitimate businesses who monitor, report, and pursue fraudulent advertisement and impersonation through current practices. As Ofcom rightfully recognises, businesses face significant reputational and financial costs while experiencing cumbersome reporting processes and delays in takedown practices. This is significantly harder for smaller companies.

For these reasons, we overall consider the proposed burden to be justified and proportionate and further encourage Ofcom to ensure that proportionality considerations do not result in weaker protections where platforms have the technical capability and resources to take effective action.

Volume 2: Risk, Governance and Control

Advertising intermediaries

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

in circumstances where they have insufficient control? Please provide any arguments and supporting evidence.

We support the principle that providers should not be able to avoid responsibility simply because parts of their advertising supply chains are operated by intermediaries. Where a provider lacks sufficient direct control, it should be required to use "all reasonable endeavours" to secure an equivalent outcome through those intermediaries. Given the potential commercial and reputational harm that fraudulent advertising can cause brands, as well as the harm it can cause consumers, a stronger "best endeavours" standard for implementing the measures should be considered.

The moderation example is appropriate: where a provider cannot directly access a reported advertisement served through an open-display supply chain, it should maintain effective arrangements with intermediaries to investigate the report and prevent the fraudulent advertisement from continuing to appear. We also strongly support the account-verification example, including checks that an advertiser genuinely works for, or is authorised by, the organisation it claims to represent.

Accountability through the supply chain. We encourage Ofcom to apply the "all reasonable endeavours" standard robustly. Complex advertising supply chains should not create accountability gaps, particularly where providers can exercise commercial leverage through their contractual relationships with intermediaries.

Know Your Business Customer controls. The Code should set stronger and more explicit expectations for "Know Your Business Customer" (KYBC) checks. Platforms should be required to apply meaningful KYBC controls before permitting advertisers to place paid-for advertisements. Advertising intermediaries must ask business customers to provide certain identification data before offering services.
At a minimum, proportionate KYBC checks should include, where relevant:

1. verifying the advertiser's legal identity and business registration;
2. verifying contact details and the country of establishment;
3. confirming that the payment method is consistent with the declared business;
4. conducting periodic re-verification rather than relying solely on one-off onboarding checks; and
5. applying enhanced scrutiny to newly created accounts, high-velocity campaigns, recently registered domains and repeat policy evaders.

Regulatory responsibility. Where a platform fails to use all reasonable endeavours to implement meaningful KYBC controls, apply appropriate "take down and stay down" measures, and improve its systems in response to repeat offending and complaints data, and that failure contributes to foreseeable harm, the platform should be held accountable under the regulatory framework.

Fraud indicator assessment

8. **Do you agree with our proposal? Please provide any arguments and supporting evidence.**
9. **Do you think there are other information sources providers should consider in order to understand how fraudulent advertising manifests on their service? If so, what information and why would they need to consider it?**

We support the proposal and welcome the requirement for providers to draw on multiple sources of evidence. These should include moderation outcomes, advertiser and account data, user reports, trusted flaggers, external experts, retrospective incident analysis and relevant data-sharing schemes.

Ofcom should also recognise rights holders and brand-protection experts as important external sources of intelligence and expertise. They can identify emerging patterns of brand impersonation, counterfeit advertising, repeat offending and coordinated activity that may not be apparent when a platform assesses advertisements individually.

We support a more explicit, proactive framework, similar in principle to the risk-assessment and mitigation approach under the EU Digital Services Act. The Code should require platforms not only to identify indicators of fraud, but also to assess systemic risks within their advertising systems and implement proportionate mitigation measures.

At a minimum, platforms should assess risks arising from:

1. weaknesses in advertiser onboarding and verification;
2. recommendation, targeting and optimization systems that may amplify fraudulent advertising;
3. commercial incentives that may discourage robust enforcement;
4. repeated impersonation of brands and individuals;
5. advertising for counterfeit or deceptively presented products; and
6. the use of generative AI to create, adapt or scale fraudulent advertising content.

Platforms should document these mitigation measures and review and update them regularly as risks evolve. A purely reactive model is no longer sufficient.

Governance and accountability

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

Yes. We strongly support Ofcom's governance and accountability proposals, particularly the requirement for a provider's most senior governance body to conduct and record an annual review of how fraudulent advertising manifests on the service, the effectiveness of the measures in place and the lessons learned.

We also strongly **support the designation of a named individual** with responsibility for compliance decision-making and accountability to the provider's most senior governance body. Clear senior-level ownership should ensure that fraudulent advertising is treated as a strategic risk, rather than solely as an operational moderation issue.

That individual should translate this accountability into practice by fostering an appropriate compliance culture, ensuring that staff receive relevant, role-specific training and overseeing the consistent implementation and maintenance of effective checks for fraudulent advertising.

For businesses frequently affected by counterfeit and impersonation advertising, effective governance must also drive continuous improvement. **Recurring patterns, repeat offenders and weaknesses identified through complaints or engagement** with rights holders should lead to improvements in platform systems, rather than the repeated removal of individual advertisements without addressing their underlying causes.

To demonstrate that these governance arrangements are working in practice, we also support **transparency obligations** that enable Ofcom to assess the effectiveness of platform measures. Descriptions of processes alone are not sufficient.
Platforms should therefore retain and, where appropriate, provide Ofcom with information on:

1. the volume of advertisements rejected, removed or restricted because of suspected fraud;
2. the time taken to act on identified or reported fraudulent advertisements;
3. recurrence rates following enforcement action;
4. the number of repeat offenders identified and blocked;
5. the application and outcomes of KYBC controls; and
6. the categories of fraud most frequently identified.

Together, these requirements would shift the framework from formal compliance towards demonstrable and measurable effectiveness.

Testing advertisement generation tools

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

We support Ofcom's proposal requiring providers to test advertisement generation tools to identify whether, and how, they could be used to create fraudulent advertisements, including testing before deployment, and at appropriate intervals thereafter.

This is particularly important as generative AI lowers the barriers to producing convincing brand impersonation, counterfeit advertising and other fraudulent content at scale. We therefore welcome the expectation that testing should lead to practical mitigations where

risks are identified, additional safeguards are needed or, even leading to cases where, if necessary, deployment is paused.

We welcome Ofcom's recognition that AI is reducing the cost and increasing the scale of fraudulent advertising. Looking ahead, these challenges are likely to intensify as AI-generated content becomes more sophisticated and AI assistants and agentic systems become increasingly embedded in online commerce. It will therefore be important to ensure that the regulatory framework remains capable of addressing both AI-enabled fraud and the growing role of AI in how consumers discover, evaluate and purchase products and services.

Volume 3: Ensuring account integrity

Account checks and actions

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

a) verification that advertising account holders work for, or on behalf of, the individual or organisation they are advertising;
b) checks and actions to prevent banned advertising account holders returning; and
c) checks for accounts with indicators that there is a material risk they will post fraudulent advertising so that restrictions can be applied to them.
d) repeat checks where there are relevant changes identified on an account.

We strongly support the introduction of a verification requirement. Luxury brands are frequent targets of impersonation and counterfeit advertising. Stronger checks before advertisements reach UK users should reduce opportunities for fraudulent actors to misuse established brands and IP to create an appearance of legitimacy.

We also welcome measures addressing repeat offenders and circumvention. Fraudsters often recreate accounts, use other existing accounts, or take over legitimate accounts following enforcement. Effective account-level measures are preferable to repeatedly removing individual advertisements while allowing the actors responsible to continue operating.

We strongly encourage providers to make appropriate use of rights-holders and trusted-flagger intelligence when conducting these checks, particularly where they can be used to identify linked accounts, repeat infringers, or patterns of brand impersonation that may not otherwise be apparent.

The Code should set stronger and more explicit expectations for "Know Your Business Customer" (KYBC) checks. Platforms should be required to apply meaningful KYBC controls

before permitting advertisers to place paid-for advertisements. Advertising intermediaries must ask business customers to provide certain identification data before offering services. At a minimum, proportionate KYBC checks should include, where relevant:

1. verifying the advertiser's legal identity and business registration;
2. verifying contact details and the country of establishment;
3. confirming that the payment method is consistent with the declared business;
4. conducting periodic re-verification rather than relying solely on one-off onboarding checks; and
5. applying enhanced scrutiny to newly created accounts, high-velocity campaigns, recently registered domains and repeat policy evaders.

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

Where risk indicators are present, providers should verify not only an advertiser's identity, but also its entitlement to use the relevant brands, trademarks, domains or other commercial assets.

In cases of impersonation or counterfeiting, establishing that an advertiser is a genuine person or business is insufficient; providers must also determine whether it is authorised to promote the brand or product concerned. This would align with existing industry practice, under which some platforms require advertisers using third-party brands or trademarks to demonstrate that they are the brand owner or an authorised promoter.

Verification must be supported by effective action against repeat offenders. Removing a single advertisement is insufficient if the same actor can immediately return through a new account, domain, payment instrument or affiliated business identity. The Code should therefore establish a clear "stay-down" expectation.

To meet this expectation, platforms should be required, on a best-efforts basis, to take reasonable technical and organizational measures to prevent the reappearance of:

5. advertisers previously identified as fraudulent;
6. identical or materially similar fraudulent advertisements;
7. linked accounts or networks associated with previous fraud; and
8. repeated brand-impersonation campaigns and counterfeit offers.

If a platform fails to use best efforts to implement such measures, and fraudulent activity repeatedly reappears despite being reasonably foreseeable and technically addressable, that failure should be taken into account when assessing the platform's compliance and liability.

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

Countering account takeover

15. Do you agree with our proposals? Please confirm which proposed measure your views relate to and provide any arguments and supporting evidence.
16. Do you have any evidence about account takeover that could inform our assessment, including how frequently it occurs or its impact?

Advertising bans

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

Yes. Account-level advertising bans are important because removing an individual fraudulent advertisement does not prevent the advertiser in question from placing new ones.

We therefore support requiring providers to take reasonable steps to prevent banned advertisers from returning through new, existing or compromised accounts. Given the persistence of counterfeit and brand-impersonation activity, providers should also use intelligence from rights holders and trusted third parties to identify links between banned advertisers and other accounts.

The Code should reinforce this obligation with a clear "stay-down" expectation covering attempts to reappear through alternative accounts, domains, payment instruments or affiliated business identities.

On a best-efforts basis, platforms should take reasonable technical and organizational measures to prevent the reappearance of:

1. advertisers previously identified as fraudulent;
2. identical or materially similar fraudulent advertisements;
3. accounts or networks linked to previous fraud; and
4. recurring brand-impersonation campaigns and counterfeit offers.

A platform's failure to use best efforts to prevent reasonably foreseeable and technically addressable recurrence should inform the assessment of its compliance and liability.

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

Account appeals

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

Yes. Legitimate advertisers should have a clear mechanism to challenge decisions, submit additional information and secure the prompt correction of errors. However, the appeals process must not provide fraudulent actors with an easy means of delaying or circumventing enforcement. Where an appeal is upheld, providers should reverse the action promptly; where evidence of fraud or material risk remains, appropriate user protections should stay in place.

Volume 4: Moderation

Advertising moderation

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

Yes. We support the proposals, but a framework that relies too heavily on post-publication notice and takedown will be insufficient. Fraudulent advertising is fast-moving, cross-border and highly adaptive, while counterfeit and brand-impersonation advertisements can be deployed at scale for short periods. Slow review or removal may therefore allow significant consumer harm before enforcement action is taken.

Effective protection requires upstream controls before advertisements are served, alongside rapid reactive removal. Moderation systems should also identify patterns of repeat infringement and coordinated activity, rather than assess advertisements solely in isolation.

Terms of service and publicly available statements

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

Yes. We support the proposal, particularly the requirement for providers to explain what proactive technology they use to comply with the fraudulent advertising duties, when it is used, and how it operates.

We also support the requirement that this information is clear and accessible, including consideration of findability, layout, language and usability. Greater transparency should help users, advertisers and rights holders understand how platforms seek to identify fraudulent advertising and provide an additional layer of accountability.
As these technologies evolve, particularly through greater use of AI, we would encourage providers to keep these statements meaningfully up to date. Transparency should be sufficiently informative to enable scrutiny of platform approaches without requiring disclosure at a level that could enable fraudulent actors to circumvent detection systems.

Advertising complaints

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

Yes. We strongly support these proposals, particularly the requirement for complaints about suspected fraudulent advertisements to feed directly into moderation processes, enabling swift assessment and, where appropriate, removal.

We particularly welcome the proposal for dedicated reporting channels for trusted flaggers. Providers should use the flexibility proposed by Ofcom to establish dedicated channels for rights holders and recognised brand-protection specialists with demonstrated expertise in counterfeit and impersonation activity. Rights holders can provide highly reliable evidence of unauthorised use of their intellectual property and help identify repeat offenders, linked accounts and coordinated activity.

Ad libraries

23. Do you agree with our proposal? Please provide any arguments and supporting evidence.
24. Do you agree with the principles, functionalities and information categories which we have included in the proposed measure? Please explain your reasoning and, if possible, provide supporting evidence.
25. Do you have any evidence or insights on the process of building an ad library from scratch or adjusting an ad library to align with the proposed measure, and how long that process would take?