Consultation response

Field	Value
Responder	Online Safety Network
Responder Type	organisation
Org Role	Director
Org Type	Civil society

Volume 1: Context

3. Online advertising ecosystem

Q1: Is there any information or evidence you hold that could enhance our understanding of the online advertising ecosystem?

We refer Ofcom here to the summary document on our website, and related supporting links.https://www.onlinesafetynetwork.uk/analysis/response-to-ofcom-consultation-fraudulent-ads/We provide the text of that summary here:
Ofcom comprehensively details the scale of online fraud and fraudulent ads/scams in its documentation to support its codes. This has increased significantly since the OSA received Royal Assent in 2023 and since the duties on fraudulent ads were added to the then (draft) Online Safety Bill back in 2021. Despite the challenges for existing regulators being known at the time - and the FCA itself calling for action on online fraud - the then Government excluded "paid-for advertisements" from the initial draft Bill. The OSA's fraudulent advertising duties were only included in the regime after a successful campaign, involving consumer groups, financial sector organisations and mental health charities, backed by the City of London Police and with pressure brought to bear directly on the Government from the FCA. While the introduction of the OSA duties relating to fraudulent adverts are welcome, definitional problems in the legislation itself may well impact on the duties' effective enforcement: we have set these out in detail here. The scope of the duties and timeframe for their implementation is also a concern.

The duties are contained in Chapter 5 of Part 3 to the OSA: they apply to two categories of regulated services - category 1 (large user-to-user platforms) and category 2A (large search services); the threshold definitions for these two categories were set out in regulations by DSIT, based on Ofcom's advice, which came into force in February 2025. (Ofcom's advice on these thresholds was itself contentious as it excluded "small but risky" platforms - see our briefing here - and the Government's regulations were then subject to a legal challenge which delayed the introduction of these phase 3 duties by at least 12 months.) The duties themselves are unlikely to be in force until the second half of 2027.
Given the fact that the duties apply only to large platforms - as per Ofcom's register of categorised services - and have been delayed for so long, it is vital that the proposed codes of practice are as robust as they can be to address the scale of harm (and losses) being experienced by British consumers. (Figures from Revolut detailing some of the platforms where scams are increasing rapidly are instructive here; and it is notable that one of those with the highest increases in prevalence, Telegram, is not covered by these duties.)
The robustness of the codes is also vital as the same concerns about compliance and enforcement apply here as to the illegal harms and protection of children's codes: platforms only have to follow the measures in the codes to be in compliance with their duties under the Act. So, for example, if their risk assessment identifies multiple areas of risk relating to fraudulent ads that do not have a corresponding measure in the codes, they do not need to address those risks; if Ofcom does not feel that they can provide a measure that

is "clear and detailed" enough for inclusion in the codes, then it gets overlooked; and the OSA's "safe harbour" means that companies can be in compliance with their duties just by following whatever is in the codes. In addition - though this is the inevitability of the regulatory regime which Ofcom is enforcing - these codes, as Ofcom says, are just "the first iteration" and will need to be updated as new evidence or new risks emerge. '

There is a lot, therefore, riding on the successful implementation of these first set of codes. Regulated services have not done enough to address the scale of scams via fraudulent ads on their platforms, and the scale of the impact has been evidenced by recent research from Public First, with real impacts for trust (and consequently spend) in the UK economy: 75% of UK adults say the presence of scam ads make them less trusting of online advertising generally and 72% are more cautious about spending money online. Moreover, as recent Reuters reporting has shown, platforms such as Meta make significant profits from carrying such ads and it is therefore unsurprising that only 37% of the UK public think action is likely to be taken when scams are reported. UK Finance has recently reported on the "industrial scale" of online fraud, and called it a threat to national security; and Trading Standards has already been flagging the risk to UK consumers of being scammed via engagement with AI-generated content, along with the City of London detailing risks relating to AI-deepfakes and cloning. Recruitment scams are an increasing source of concern for the police; and fraudulent ads are not just linked to financial losses for individuals but the risk of harm from unsafe or dangerous products; see for example, evidence from the MHRA and ASA.

Ofcom's codes need teeth if they are to make a difference. We therefore welcome the fact that the measures provided in these draft codes are, in the main, those which expert stakeholders such as Which? have been calling for for many years and we draw on their analysis and recommendations for further improvements in our detailed response below.

The Codes alone are not enough if Ofcom is not going to effectively enforce them. To date, there has been no enforcement action against platforms in relation to their duties under the illegal harms codes to take action on fraud as a criminal offence and Ofcom did not make fraud or fraudulent ads a priority for this year's activities. This has to change: notwithstanding the pressures on Ofcom at present and the strain on their resources arising from the implementation of the social media ban, consumers have been let down for many years by platforms, regulators and policymakers turning a blind eye to the scale of fraudulent activity and scams on online platforms. When these codes of practice finally come into force, Ofcom needs to signal a zero tolerance approach to their enforcement. We will continue to call on the Government to amend the Online Safety Act to improve Ofcom's scope for tougher implementation and enforcement.

4. Causes and impacts of fraudulent advertising

Q2: 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.

Ofcom's assessment is comprehensive and robust. We also refer Ofcom to the additional evidence provided by Which? in their submission which provides further detail and insight on the way in which scammers operate online and the scale of risks and losses to consumers.

Q3: Do you agree with the examples of risky characteristics we have provided? Please provide any arguments and supporting evidence.

No response

5. Our approach to developing Codes measures

Q4: Do you agree with our proposed approach? Please provide any arguments and supporting evidence.

We welcome the fact that Ofcom is prioritising an upstream approach, aiming to prevent the posting of fraudulent advertisements in the first place, to improve the speed at which fraudulent advertisements are

detected, and to ensure swift action to remove fraudulent advertisements once they are detected. This is much more preferable to an approach focusing solely on downstream measures, such as content moderation or takedown - which are also included in the code measures - as often the harm has been caused by that point. In the case of fraudulent ads, that often means that a user - or multiple users - who have been tricked by the ad will have lost money and the harm is quantifiable.

We have consistently argued in our responses to Ofcom's previous OSA implementation measures that a combination of both upstream and downstream measures is vital and, in the case of these particular proposals, it is welcome that Ofcom's approach is more closely aligned with one based on "safety by design"

We support the proposal that in-scope services use proactive technology to detect fraudulent advertisements, and that Ofcom will propose a proactive technology measure for the fraudulent advertising code in autumn 2026. The introduction of this, in tandem with the account-level measures that Ofcom is suggesting, will provide an important layering of defences. Where scammers are able to bypass account-level checks, then the proposed measures such as proactive detection, content moderation and user reporting, backed up by bans for those found to have posted fraudulent advertisements, can ensure that fraudulent content is detected and that those posting fraudulent content are removed from platforms before they can do further harm. We understand from our partners at Which? That this approach mirrors other international approaches, including in Taiwan and Australia, and we welcome the fact that Ofcom is learning from what works elsewhere and that there may be an alignment in regulatory approaches; this is particularly important given that online fraud is often carried out by international criminal networks and fraudulent ads are generated on an industrial scale by scam factories based abroad.

6. Combined impact assessment

Q5: 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.

We believe that the overall burden on service providers to be proportionate and we point Ofcom to the analysis that Which? has provided in their evidence submission comparing the overall costs borne by consumers who encounter fraudulent advertising with the projected costs borne by the categorised services covered by these measures. Given that these services are the biggest - and most profitable - companies in this sector, there is no reason why they cannot absorb the costs related to implementing the code measures.

As Ofcom's analysis suggests that a 10% reduction in fraudulent advertising could mean a reduction in costs to UK users and the wider economy of GBP70 million a year, then the maximum estimated costs of applying Ofcom's measures (GBP60m a year) - even with a minimal impact on fraudulent advertising - will still have a positive economic benefit. The proposals are therefore justified and proportionate.

Volume 2: Risk, governance and control

2. Advertising intermediaries

Q6: Do you agree with our proposal? Please provide any arguments and supporting evidence.

We agree with this measure which is vital to the effective implementation of the fraudulent advertising codes. If there were no obligation in place for the service to pass along their moderation responsibilities to an intermediary in the supply chain, the fraudulent ads would be published and likely cause harm to consumers. If a service cannot conduct moderation of ads themselves, they must be obliged to require intermediaries with whom they work to conduct the moderation in their place.

We point Ofcom to the concerns raised by Which? about this measure, in particular in relation to the use of the phrase "all reasonable endeavours": this should be strengthened to place a requirement that services use

contractual arrangements with intermediaries to ensure that some version of the measure in question is being implemented. We note that this is an approach already required via Ofcom's Statement on Mobile Messaging Scams, which obliges mobile operators and aggregators to pass requirements (including KYC checks) through the supply chain through clear and unambiguous contractual terms and see no reason that the same approach should not be mandated here to ensure that Ofcom can go as far as it can to deliver its objective of reducing harm from fraudulent advertising.

Q7: 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.

N/A

3. Fraud indicator assessment

Q8: Do you agree with our proposal? Please provide any arguments and supporting evidence.

We agree with this proposal, including the suggested conditions for the characteristics of adverts and advertising accounts that could indicate a material risk of fraudulent advertising. Expert organisations in this space note that scammers use the same or extremely similar content to perpetrate the same scam over and over again so it is vital that platforms use the information they already hold on previous fraudulent ads or scams to make judgements on new ads that look similar.

We agree with Which?'s suggestion that the first condition proposed by ofcom should also include content that has been used in fraudulent advertisements on any service, given the way in which scammers operate across multiple platforms often reusing similar content or approaches. We also agree with their recommendation that the measure referring to "information received via data sharing schemes" should be revised to "information from data sharing schemes": services should have to actively seek out threat intelligence to help inform their fraud impact assessment.

Q9: Do you think there are other information sources providers should consider in order to understand how fraudulent advertising manifests on their service? If so, what information and why would they need to consider it?

N/A

4. Governance and accountability

Q10: Do you agree with our proposals? Please confirm which proposed measure your views relate to and provide any arguments and supporting evidence.

N/A

5. Testing advertisement generation tools

Q11: Do you agree with our proposal? Please provide any arguments and supporting evidence.

N/A

Volume 3: Ensuring account integrity

2. Account checks and actions

Q12: 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 :

Yes. We provide comments on the specific proposals below.

Q12.A: verification that advertising account holders work for, or on behalf of, the individual or organisation they are advertising

We agree with this measure which is vital to the effectiveness of the fraudulent advertising codes and point Ofcom to Which?s evidence in support of it.

Q12.B: checks and actions to prevent banned advertising account holders returning

We agree with the position that Ofcom is taking that the effectiveness of advertising bans depends on how easily bad actors can evade them and point Ofcom to Which?s evidence in support of it. This specifically shows how fraudsters commonly change the account name, and how changing phone numbers and email addresses is not a major obstacle for fraudsters.

We support Which?;s point that, if platforms are only required to collect information that is easy for fraudsters to change, then they will be able to hide behind the safe harbour provisions of the codes to claim compliance with their duties. We recommend - as Which? Argues - that the duty under FAU/FAS H1.3 (b) (i) in the draft code should read "collecting all reasonably available relevant information about the person using, or intending to use the account" rather than "collecting any relevant information about the person using, or intending to use, the account." We also support their call that, as a minimum, services should have to collect contact details (name, address, telephone number), a copy of an identification document (such as a passport or official ID card), and payment account details, which would align the fraudulent advertising codes of practice with requirements outlined under Article 30 of the Digital Services Act.

Q12.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

We point Ofcom to Which?'s evidence in support of this measure, which details examples of fraudulent accounts, with very obvious red flags, which platforms should have applied restrictions to in the past. This proposed measure, if properly implemented and enforced, has the potential to restrict the ability of fraudsters to target consumers at scale.

Q12.D: repeat checks where there are relevant changes identified on an account.

Again, we point Ofcom to the evidence provided by Which? which supports the need for such a measure: platforms have a weak track record when it comes to conducting checks on existing accounts that exhibit signs of suspicious behaviour or account takeover which fully justifies the need for Ofcom's proposed measure. As Which? States in its evidence, "it is clear that, in the absence of strong regulatory incentives, platforms will not take the requisite action to verify the legitimacy of accounts exhibiting suspicious behaviour".

Q13: 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.

N/A

3. Preventing fraudulent financial services advertising

Q14: Do you agree with our proposal? Please provide any arguments and supporting evidence.

We support this proposal, particularly given increasing prevalence and widespread harm caused by investment scams and urge Ofcom to implement all the specific mechanisms proposed. Which? has provided evidence to support the importance of services verifying that advertisers are either FCA-authorised or not on the FCA warning list, as well as the importance of services using proactive detection to identify financial services adverts, which we urge Ofcom to take account of.

4. Countering account takeover

Q15: Do you agree with our proposals? Please confirm which proposed measure your views relate to and provide any arguments and supporting evidence.

We agree with Ofcom's proposals here and, again, point to the evidence Which? Has already provided to Ofcom. We also back their calls for Ofcom to specify a more robust measure for account security mechanisms due to the risk of MFA via one-time passcodes being susceptible to being compromised. Which? has written extensively about how one time passcodes leave consumers vulnerable to account compromise and we also agree with them that it is extremely unlikely that categorised services will not be able to use a stronger method than message based two-factor authentication. We would like to see Ofcom including a statement in their guidance that message-based authentication is not likely to be sufficient to comply with measures FAU/FAS H3.

Q16: Do you have any evidence about account takeover that could inform our assessment, including how frequently it occurs or its impact?

N/A

5. Advertising bans

Q17: Do you agree with our proposal? Please provide any arguments and supporting evidence.

We agree with measures FAU H5 and FAS H5 and refer Ofcom to Which?s evidence in support of these

Q18: Are you aware of any additional exceptional circumstances in which it may be proportionate for providers to reverse advertising bans?

N/A

6. Account appeals

Q19: Do you agree with our proposals? Please confirm which proposed measure your views relate to and provide any arguments and supporting evidence.

N/A

Volume 4: Moderation

2. Advertising moderation

Q20: Do you agree with our proposals? Please confirm which proposed measure your views relate to and provide any arguments and supporting evidence.

We agree with the proposals for effective advertising moderation functions and point Ofcom to Which?'s assessment of each of the proposals which they provide in their evidence. We would in particular highlight our support for the following recommendations:

A specific statement in the codes of practice that platforms would not rely solely on user reporting but also include reference to the use of automated technology and trusted flaggers as means to detect suspected trusted flaggers.
The inclusion of a specific timeframe for the removal of fraudulent advertising content when it is reported to a service. As Which? notes, even a short delay in removing a fraudulent ad can lead to thousands of additional consumers being exposed to it. We support their recommendation that services should have to remove fraudulent adverts within 24 hours of assessing that the advert is fraudulent.
The requirement on providers to publish a report detailing their targets and their performance against the targets. This would create more transparency and allow civil society organisations and other interested parties to point out where services were deliberately setting weak targets in order to protect revenues at the expense of removing illegal content.

3. Terms of service and publicly available statements

Q21: Do you agree with our proposals? Please confirm which proposed measure your views relate to and provide any arguments and supporting evidence.

N/A

4. Advertising complaints (including DRC for trusted flaggers)

Q22: Do you agree with our proposals? Please confirm which proposed measure your views relate to and provide any arguments and supporting evidence.

We support all these proposals and, again, point Ofcom to the evidence provided by Which? In support of some of the specific measures and their view that, if properly enforced, these measures will be impactful.

5. Ad libraries

Q23: Do you agree with our proposal? Please provide any arguments and supporting evidence.

Ad libraries are vital for scrutiny of online platforms; many of the civil society organisations we work with rely on them to carry out their work across a wide range of harms. It is vital therefore that this measure is as robust and comprehensive as possible to allow this work to continue.

We therefore welcome this proposal but support the calls made by Which? for some clarifications and amendments to be considered before the final version is included in the codes. These include:
Specifying in measures FAU/FAS E1.3 that access to ad libraries "should be available without the need to register or login to access, including where APIs are used."
The addition of a requirement for services provide a mechanism for users to report when ad libraries are not functioning as expected, so that services can address issues quickly when they arise.
Clarifying that the name of the advertiser should always be visible, even if the ad was taken down or the user banned.
Mandating that platform ad libraries disclose the ultimate paying entity and primary financial beneficiary of an advertisement, in addition to simply the agency or account holder placing the ad on their behalf. This would enable researchers and enforcement agencies to link seemingly isolated scam accounts, track rogue affiliate networks and disrupt fraud operations at scale.
Specifying more clearly the groups of UK users the ads are targeted, amending the existing wording to read: "the particular groups of UK users the ad is targeting, whatever the basis for that group being targeted may be." This will prevent platforms from only enabling search on the basis of specific predefined characteristics, such as age or gender, and will make ad libraries more useful as a result.
Providing metrics on both the number of UK users the relevant ad is targeting AND the number of UK users who have encountered the ad. At present, the requirement is for one or the other: both of them provide

different insights and are therefore useful for researchers and campaigners. The number should also be precise, rather than given as part of a range, as ranges are far less useful in terms of understanding the harm, particularly at the lower end.
Including not only how many UK users encountered an ad, but the number of UK users who interacted with an ad (i.e. by clicking on an embedded link). This will enable researchers to better understand the impact of a fraudulent ad, as they can see how many consumers were drawn in by the ad versus those that ignored or did not register it, improving the usefulness of ad libraries overall.

We support Which's preference that platforms clearly label ads that were taken down (as opposed to ads whose run simply expired) and provide the exact reason an ad was taken down (i.e. the precise legal or policy violation cited by the platform). As Which? Set out, this will not just help civil society organisations, Ofcom, and other regulators to understand which fraud offences are easier for platforms to infer when conducting advertising moderation but it will also inform future thinking about any changes to the Online Safety Act in the future, or whether Ofcom needs to revise its Illegal Content Judgement Guidance.

We also recommend that the daily data updates should include all adverts uploaded within a given 24-hour period, even where these have been deleted before the end of that period; and that there should be additional search criteria included so that users can make more granular searches, with a view to ad libraries being easier to use, increasing transparency and thereby consumer protection from fraudulent ads.

For the reasons set out by Which? In its submission, it is essential that ad libraries include the links embedded in ads, as doing so will make it easier for researchers to find more fraudulent ads and will increase consumer protection overall as a consequence. In addition, we support their calls for ad libraries to preserve ads for 5 years after they stopped being live on the service (rather than the one year currently proposed), given that the same scam can often recur over several years.

Q24: 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.

N/A

Q25: Do you have any evidence or insights on the process of building an ad library from scratch or adjusting an ad library to align with the proposed measure, and how long that process would take?

N/A

Additional questions

Q26: Do you agree with our Equality Impact Assessment? Please provide any arguments and supporting evidence.

N/A

Q27: Do you agree with our Welsh language assessment? Please provide any arguments and supporting evidence.

N/A

Q28: Do you agree with our proposals? Please provide any arguments and supporting evidence.

We agree with the proposals set out by Ofcom for the updates to the ICJG and particularly support the intention to add some additional 'red flag indicators' to the existing list of examples of fraud by false representation contained within the ICJG.