Consultation response

Field	Value
Responder	Which?
Responder Type	organisation
Org Role	Senior Policy Advisor
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?

No response

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.

No response

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.

Yes. As outlined in Volume 1 of the consultation document, Ofcom aims to stop fraudsters posting 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.

Ofcom is proposing a layered approach, consisting of upstream and downstream measures. Ofcom's proposed upstream measures consist of account level 'safety by design' interventions to stop fraudsters advertising from the outset and to address the scale and speed at which fraudulent advertising happens. Ofcom's proposed downstream measures include measures on moderation and reporting to ensure that those fraudulent advertisements which make it through are detected and removed.

Which? supports this approach, as services will need to deploy both downstream and upstream measures to effectively prevent fraudulent advertising. Downstream measures alone will not be sufficient to achieve Ofcom's objectives, especially the objective to prevent fraudulent advertisements from being posted in the first place. However, upstream measures alone will not be one hundred percent effective, meaning that downstream measures will be required to remove those fraudulent advertisements that do make it through

the account-level checks.

An approach focused solely on reactive moderation and reporting will not be sufficient. As we argued in our response to Ofcom's consultation on Online Safety - Additional Safety Measures, fraud victim reporting rates are very low, with most reports going to the victim's bank rather than to the platform which hosted the fraudulent content. Any approach that relies solely on reporting and reactive moderation will therefore only capture a small minority of overall fraudulent content, and will not meaningfully reduce online fraud in the UK.

We appreciate that Ofcom has proposed 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. In our response to Ofcom's consultation on Online Safety - Additional Safety Measures, we shared our support for the use of proactive technology. Our research has shown that proactive technologies can be effective in identifying potentially fraudulent content. However, even the best proactive technology will never capture all of the potentially fraudulent content on any given platform. That is why it is important to add an additional layer of defence - the account-level measures that Ofcom has suggested.

Having said this, it is also clear that some scammers will be able to pass account-level checks. For example, Which? has reported that scammers can use deepfake videos to pass certain identity verification checks. This does not mean that platforms should not have to introduce account-level checks, but it does mean that a defence in depth strategy such as that being proposed by Ofcom is the best way to achieve the regulator's objectives. In cases where scammers are able to bypass account-level checks, 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.

Other countries have adopted a layered approach similar to the measures proposed by Ofcom with some success. Taiwan's Fraud Crime Hazard Prevention Act requires online advertising platforms to implement identity verification for advertisers and to remove or restrict access to fraudulent ads within 24 hours of receiving a notification from regulatory or law enforcement authorities. According to Taiwan's publicly-available national fraud dashboard, there has been a general downward trend in both fraud volume and fraud losses since full enforcement of the Fraud Crime Hazard Prevention Act started in January 2025.

Australia's Scams Prevention Framework, which came into force in February 2025, takes a similar layered approach. Regulated sectors, including digital platforms, must adopt advertiser verification for certain products, maintain automated, real-time monitoring to identify fake ads and compromised accounts, and take prompt action to remove fake ads and the accounts posting them. Investment scam losses in 2025 were AUD $837.7, down from AUD $945 in 2024, while the median loss per victim fell from AUD $500 to AUD $400 across the same period. Recent data shows a 17% decrease in online fraud losses for Q1 2026 compared to Q1 2025.

Overall, it is clear that no single method is 100% effective at stopping fraud and fraudsters, meaning that a layered approach such as that proposed by Ofcom is necessary. Moreover, there is evidence from other countries that layered approaches can be effective at reducing both the volume of fraud cases and the overall value of fraud losses. We therefore support Ofcom's approach.

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.

Yes. The costs borne by consumers who encounter fraudulent advertising are much higher than the projected costs borne by categorised services to implement Ofcom's proposed measures. Therefore, we do consider the overall burden on the service providers in scope of Ofcom's proposed measures to be proportionate, especially bearing in mind the particular statutory factors on proportionality in the OSA (In

section 38(5) and section 39(6)) on nature and severity of harm caused by fraudulent advertisements, which our evidence has extensively demonstrated.

The Home Office's 'Economic and Social Cost of Crime' reports consider three main cost areas in relation to fraud: costs in anticipation of fraud; costs as a consequence of fraud; and costs in response to fraud.

Costs in anticipation of fraud are costs incurred to prevent incidents of fraud from occurring. These are most likely to be borne by businesses which fraudsters use to target individuals, such as financial services institutions. According to the latest Economic and Social Cost of Crime report, costs in anticipation of fraud account for around 10% of the overall social and economic cost of fraud against individuals.

Costs as a consequence of fraud are the financial losses and emotional harms incurred by victims of fraud following an incident of fraud. The Home Office estimates that costs as a consequence of fraud account for 78% of the overall cost of fraud against individuals.

Costs in response to fraud are costs incurred to investigate, enforce and operate the legal system and other institutions in fraud cases. These costs consist of policing and enforcement costs, judicial service costs, and costs borne by the financial services industry. The latest Home Office report estimates that costs in response to fraud account for around 12% of the total overall social and economic cost of fraud.

The Home Office's analysis indicates that the cost of fraud against individuals is borne disproportionately by individuals and by society more widely. Ofcom estimates the financial losses suffered as a result of fraudulent advertising to be between GBP206 million and GBP222 million each year. Using Which? research which provides a financial estimate for the wellbeing damage caused by fraud victimisation, Ofcom has also estimated the monetary impact of reduced wellbeing (i.e. emotional harms) at between GBP193 million and GBP215 million each year. This gives a total cost as a consequence of fraudulent advertising of between GBP399 million and GBP445 million a year. It is worth noting that these figures - per Ofcom's analysis - are considered to be underestimates of the true total cost.

There are likely to be further costs as a consequence of fraudulent advertising that Ofcom has not identified. These include costs incurred due to time taken off work because of the fraud incident, costs incurred due to reduced productivity because of the emotional harms sustained from the incident, costs incurred by the NHS and other healthcare providers of responding to the physical and emotional harms of crimes, and costs incurred by the National Economic Crime Victim Care Unit. These costs are estimated in the aggregate in the Home Office Economic and Social Cost of Crime report, but we do not have specific numbers for them in relation to fraudulent advertising. However, if we assume that these costs do not differ significantly whether they are incurred as a result of fraudulent advertising or another kind of fraud, based on the Home Office's estimates, the cost of lost output, health services and victim services are likely to range from GBP156 million per year to GBP174 million per year.

There are also likely to be further costs which are somewhat intangible, or difficult to estimate at this moment. For example, on top of the social and economic costs already discussed, scam victimisation can have broader negative economic consequences. Which? has found that 73% of those who have experienced scams (either first hand or via a friend/family member) tend to choose established brands when looking for goods and services as a result of having been scammed. This risks market concentration and squeezing smaller businesses out of markets, which may impose costs on the wider economy and on consumers in the long term. Another category of potential costs to society includes the opportunity cost of losses, such as missed investment opportunities or further impacts on consumption levels of individuals. The Economic and Social Cost of fraud report discusses these costs, but does not provide an estimate for them.

By contrast, Ofcom estimates that the likely maximum cost to a service of implementing its proposed measures is GBP4 million per year. There are only 15 services in scope, meaning that the maximum estimated cost of the measure is GBP60 million per year. In reality, the cost is likely to be much lower, both because not all categorised services will need to deploy the measures to their fullest extent, and because many of the categorised services are owned by the same parent company, meaning that the company can

benefit from economies of scale when rolling out the measures across different services. Moreover, some providers will already have similar measures in place to tackle fraudulent advertising, meaning that the likely incremental costs associated with the proposed measures will be more modest than the above estimates suggest, as Ofcom acknowledges.

Ofcom's proposed measure seeks to increase the costs borne by regulated services in anticipation of fraud in order to reduce the costs as a consequence of fraud and the costs in response to fraud. 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. If we accept the maximum estimated cost of applying Ofcom's measures (GBP60 million a year), we can see that even if Ofcom's measures only produce a modest reduction in fraudulent advertising, they will still produce a positive economic benefit overall. Therefore, given the disproportionate way in which costs currently fall on consumers, and the fact that even a relatively modest reduction in fraud will result in a net benefit to the economy and society overall (based on Ofcom's assumptions), Which? believes that Ofcom's measure is 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.

Ofcom is proposing that, where a provider cannot implement a measure, in whole or in part, due to the degree of control that it has in relation to the placement of paid-for advertisements on the categorised service, that providers should use all reasonable endeavours to implement a version of the measure that is as similar to the measure as possible. Ofcom is proposing this because, in some cases, providers may use advertising intermediaries in an open display supply chain, and may not therefore have the same degree of control as providers which manage the entirety of the supply chain themselves ('walled gardens').

In principle, Which? agrees with this measure. Our research has shown that the prevalence of fraudulent advertisements delivered via the open display supply chain is widespread. We found that some of the fraudulent ads we identified were posted by an advertiser based in Lithuania that had previously been subject to complaints about false and misleading advertising. This is the kind of detail that a service which controlled the entire advertising supply chain (a walled garden operator) should be able to identify via conducting account checks, but which may not be possible for an operator operating in the open display market to discover on their own. If there were no obligation for a service to require the intermediaries in the supply chain to conduct account checks in the service's stead, no account check would be conducted, and the fraudulent advertiser would be able to act with impunity. Therefore, it is essential that, where the service cannot conduct the account check themselves, they must be obliged to require intermediaries with whom they work to conduct the account check in their place.

A separate Which? investigation from 2026 found numerous instances of suspicious ads being promoted via the open display supply chain. These included deepfake ads featuring Richard Branson selling a diabetes product, and deepfake videos of Martin Lewis promoting a suspicious investment platform. Were similar ads to be published on a walled garden advertising service, we would expect the service in question to proactively identify them as potentially fraudulent (based on Ofcom's Illegal Content Judgement Guidance) and to remove them from the service swiftly. However, were such ads to be placed via the open display supply chain, it might not be possible for the categorised service to identify the ads as potentially fraudulent in a proactive manner. 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, thereby conflicting with the overall purpose of the fraudulent advertising duty, which is to reduce harm from fraudulent advertising. Therefore, as with account checks, it is essential that, where 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.

Which? does have some concerns about this measure. Firstly, we feel that the language around 'all reasonable endeavours' should be strengthened. At the moment, Ofcom' states that 'all reasonable endavours' "should include working with or requiring advertising intermediaries...to implement a version of the measure." In our view, the presumption should be that services use contractual arrangements with intermediaries to ensure that some version of the measure in question is being implemented. This would bring the draft fraudulent advertising codes into alignment with 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. In our view, a contractual obligation will provide a stronger incentive for an intermediary to carry out a measure assiduously (whether it is content moderation or an account check) than a non-contractual obligation. A measure that is built on contractual obligations would therefore likely prevent more fraudulent advertising than a measure built on more voluntary obligations, and would accord better with Ofcom's overall objective of reducing harm from fraudulent advertising.

We are also keen to stress that the mere presence of an intermediary in a supply chain should not be taken to indicate that a service has insufficient control to carry out a measure in the codes of practice. While we acknowledge that Ofcom may not wish to define 'degree of control' due to the highly context-dependent nature of each individual service's arrangements, we believe that Ofcom must closely monitor services' interpretation of this measure to ensure that they are not using the presence of intermediaries to abdicate their responsibilities under the codes.

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.

See above.

3. Fraud indicator assessment

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

Ofcom has proposed that providers should carry out a fraud indicator assessment to identify characteristics that indicate, either alone or in combination, a material risk of fraudulent advertising. The provider should review and update its assessment at least every 12 months or whenever the provider makes a significant change in relation to paid-for advertisements. The provider should track characteristics and groups of characteristics for the purpose of identifying any new potential fraud indicators and then assess, as soon as practicable, whether they indicate a material risk of fraudulent advertising. Which? agrees with this proposal. We address the individual aspects of the proposal in detail below.

Ofcom is proposing that providers should identify the characteristics of adverts and advertising accounts that could indicate a material risk of fraudulent advertising. Ofcom says that these characteristics should meet one or more of the following conditions: they have been previously used in fraudulent advertisements on the service or in advertising accounts that have been used to post fraudulent advertisements; they have been identified in broader fraudulent advertising trends; or the provider has other evidence to consider that they indicate a material risk of fraudulent advertising. Which? agrees with this. We often see scammers using the same or extremely similar content to perpetrate the same scam over and over again. For example, in 2022, we reported on a scam run by an advertiser calling itself 'UK Bonds Investment.' This rogue advertiser had appeared on Facebook under several different names, but the website to which its adverts linked were always identical. This highlights the importance of platforms using previous information they possess on

fraudulent adverts to make judgements about new adverts; in this case, if the service in question had reviewed the new content posted by 'UK Income Bonds' in the context of very similar content that was known to be fraudulent, it may have removed the new content sooner or not allowed it at all, thereby sparing consumers from at least some of the harm they incurred.

However, we have one recommended change to this aspect of the measure. We feel that the first condition should not only include content that has been previously used in fraudulent advertisements on the service in question, but content that has been used in fraudulent advertisements on any service. This is because we have seen the same fraudulent content crop up on different services. Throughout 2025 and 2026, we have reported on the Quantum AI scam, a fraudulent campaign advertising a fake investment firm named Quantum AI. The scammers behind Quantum AI have been able to repeatedly post new adverts on different services for the fake firm, despite platforms having previously taken down content relating to Quantum AI. If platforms proactively looked for known fraudulent content - for instance via data sharing schemes - they might have identified and prevented the Quantum AI scam from being posted on their service, thereby reducing the amount of harm the scam could do to consumers. While we acknowledge that mandating participation in data sharing agreements is outside the scope of Ofcom's powers, we feel that Ofcom's guidance should encourage platforms to use information from other services when conducting a fraud indicator assessment.

Ofcom also argues that any characteristics pertaining to fraudulent adverts or fraudulent advertising accounts should relate to: the content of the relevant paid-for ad or relevant content connected to the ad; advertising accounts; the behaviour of advertising accounts; the particular groups of users a relevant paid-for advertisement is targeting; and functionalities of the service relating to paid-for advertisements. Which? agrees with these suggestions. We believe it is important that services review not only the content of an ad but also the content connected to it, such as URLs. This is because we often see examples of ads that impersonate brands in a convincing way and where the only indicator of possible fraud is the fake website to which the ad is linked. In November 2025, we reported on scam ads which impersonated Lidl. While the ads themselves looked realistic enough, the website to which they were linked immediately raised red flags, including the fact that it was recently registered, featured no contact information or terms and conditions, and that the address on the website led to an empty car park. This is not the only such example; in March 2026, we reported on attempts by scammers to deceive consumers using imitation websites of well known brands, including Amazon, Boots, and Tesco. In these cases, focusing solely on the content of the ad itself would not have been sufficient; platforms will only be able to fully mitigate harm to consumers if they consider not only the content of ads but also the connected content, including any URLs embedded within the ad.

Which? also agrees with Ofcom's suggestion that advertising accounts and advertiser behaviour are relevant characteristics to be considered when assessing fraud indicators. In March 2023, we reported on fraudulent ads purporting to give away GBP735 worth of Lego for just GBP3. The account posting the advertisement for this offer had only five followers. In November 2025, we reported on a number of impersonation scams, including a fake Evri account which claimed to have 1.2 million followers but which in fact had zero. In October 2024, we reported on a series of fake competitions being advertised online. In most cases the profiles posting the ads were brand new, despite the fact that they purportedly belonged to established brands. If services were to treat these kinds of characteristics as indicators of possible fraud, it is possible that more such accounts will be identified and removed quickly, reducing the overall harm to consumers.

We also support Ofcom's assertion that services should consider to whom ads are targeted as a relevant characteristic for a fraud indicator assessment. We have seen examples both of wide-ranging targeting of specific demographic groups and of micro-targeting of previous fraud victims. In June 2024, we reported on an increase in cold calls targeting older people about personal healthcare devices. Given the targeted nature of online advertising, there is no reason to believe that scammers would not use similar tactics on regulated services. In November 2025, we reported on the phenomenon of 'recovery scams', where fraud victims are directly targeted by professionals claiming to be able to help them recover lost money. In both cases, details about at whom ads are targeted could provide an indicator of fraudulent activity and intent, and were

platforms to factor this information into their fraud indicator assessments, they may be able to identify, remove and prevent more fraudulent ads, improving consumer safety overall.

Ofcom has stated that providers should take into account the following information when carrying out a fraud indicator assessment: previous moderation decisions; evidence drawn from existing controls; relevant user data and advertiser data; user reports; engagement with intermediaries (to the extent that providers use them); evidence from trusted flaggers; consultation with internal experts; retrospective analysis of incidents of fraudulent advertising; product safety testing; internal and external commissioned research; outcomes from internal or external audits; and data sharing schemes. Which? believes that all of this information is potentially relevant.

Which? agrees that providers should take into account previous content moderation decisions when making a fraud indicator assessment. We have seen numerous cases of fraudulent content reappearing after having been removed by platforms. For example, we first reported on the Quantum AI scam in November 2024, having found numerous suspicious ads on Facebook and Instagram as part of the investigation. In July 2025, we reported that Quantum AI ads had begun to reappear on Meta-owned platforms. If the service in question had assiduously examined previous moderation decisions in relation to Quantum AI, it may have identified the recurring ads more quickly and prevented more consumer harm.

Which? also agrees that services should consider evidence from trusted flaggers when conducting a fraud indicator assessment. In March 2021, we reported on a spate of fraudulent investment ads on search engines. We found that many of the firms on the Financial Conduct Authority's (FCA) warning list were able to advertise on either Google or Bing. In March 2022, we reported on the case of a fraudulent advertiser under the name of 'UK Bonds Investment', which was likewise on the FCA warning list at the time. In December 2022, we reported about scammers operating under the name 'Tesler', again a name which appeared on the FCA warning list. Had the services in question consulted information from trusted flaggers such as the FCA more robustly, they might have identified these known scammers before they were able to post fraudulent content, thereby sparing consumers from harm.

Which? also agrees that services should use relevant information they receive from data sharing schemes to inform their fraud indicator assessments. We have evidence that scammers tend to operate across multiple platforms, meaning that services may have to seek data from outside their own estate in order to build the fullest-possible picture of scam indicators. For instance, in October 2025, we reported that Quantum AI scams were appearing on Google-owned YouTube, having previously appeared on Meta-owned platforms. Had the services been exchanging threat intelligence with one another, it is possible that Google would have been able to recognise Quantum AI as a scam before it was able to post fraudulent adverts, preventing harm to consumers in the first place.

However, we believe that Ofcom should amend the codes of practice to read "information from data sharing schemes", as opposed to "information received via data sharing schemes". In our view it does not suffice for platforms to be passive recipients of threat intelligence. Rather, as we argued in our response to a similar question in Ofcom's consultation on combatting mobile messaging scams, services should have to actively seek out threat intelligence to help inform their fraud impact assessment. Moreover - though we acknowledge this is beyond Ofcom's remit - we believe that it should be mandatory for services to forward intelligence on fraud actors and tactics garnered from user reports to a centralised data sharing function, perhaps modelled on the Australian National Anti-Scams centre.

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?

Please see above.

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.

No response

5. Testing advertisement generation tools

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

No response

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 :

No response

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

Ofcom has argued that where service providers verify that advertising account holders work for or on behalf of the individuals or organisations they advertise, they will likely be able to better prevent impersonation fraud. Which? agrees with this argument and supports this measure.

Our evidence shows that scammers frequently impersonate well-known brands or individuals in order to deceive consumers. Which? has reported on numerous instances of this behaviour. For example, one of the most common types of scam in 2024 was a travel scam, where fraudsters impersonated well-known transport companies such as Great Western Railway in order to deceive consumers into divulging personal information in exchange for free or heavily discounted local travel.

Brand sale scams were also one of the most common types of scam in 2024. These scams included fake giveaways of well-known brands, including iPhones and Smeg kettles. Once again, the ads included links which led to websites asking consumers to give away their personal and financial information.

In May 2025, we discovered a scam in which fraudsters impersonated supermarket Costco in order to sell fake paddling pools. The ads posted by the fraudsters funnelled traffic to multiple fake e-commerce sites.

We have also received numerous reports of impersonation scams to our Scam Alerts Service in the last few months. In July, we reported that VPN provider NordVPN had uncovered a criminal network creating Facebook and Instagram ads that impersonate trusted brands, including Google Authenticator, Disney+, Duolingo and Airbnb to advertise fake apps. Once clicked on, these ads redirected consumers to unlicensed online casinos asking for a deposit. In June 2026, consumers flagged scam ads in Google Search results impersonating Aldi and leading to a copycat website.

In all of these cases, the harm to consumers would likely have been substantially mitigated - or even entirely prevented - if platforms had verified that advertising account holders worked for or on behalf of the organisations that they claimed to represent. Given how common impersonation is as a tactic, we believe that this measure is an absolutely vital component of the fraudulent advertising code and urge Ofcom to ensure its inclusion in the final codes.

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

Ofcom has argued that the effectiveness of advertising bans depends on how easily bad actors can evade them. Which? agrees with this statement. Our evidence shows that current platform practice is not effective in ensuring that banned account holders do not return to commit fraud.

In 2021, we reported on fake shoe retailer ads which had at the time been circulating on social media for years. If the platform removed the ads, the scammers simply set up again under a different account with new ads. One victim, who had clicked on one of the ads previously, reported seeing them on a weekly basis in his feed after the initial scam, often under a new company name, suggesting that the same scammers were returning time and again.

In 2024, we reported on a known investment fraudster who had previously operated under the alias UK Income Bonds, but which at the time was operating as British Property Bonds. We had first flagged this fraudster to Facebook in December 2021, but that did not prevent the fraudster from repeatedly posting more adverts and defrauding more UK consumers. Although the name of the company associated with the scam changed frequently, the landing page behind the ad was in all cases identical.

In 2025, we became aware of a series of adverts for hearing aids circulating on Facebook. These ads used a fake Which? logo, despite the fact that the Facebook account and the website to which the ads redirected consumers were not associated with Which?. We reported the ads to Meta, who removed them after a few days. However, within a couple of months the ads had reappeared.

These examples illustrate the fact that the bans currently imposed by platforms are not effective. After being banned, fraudsters are able to post the same scam content after a few days, perhaps using a new email address and business name. We therefore agree with Ofcom's suggestion that services should collect information about holders of new advertising accounts before those accounts can post adverts to UK users, and that services should check those details against information they hold on banned users.

Ofcom states that the information platforms may collect includes: contact details, metadata, and payment details. Ofcom also states that service providers may decide to carry out identity verification checks. In our view, simply collecting contact information will not suffice. As our above examples demonstrate, fraudsters commonly change the account name, and changing phone numbers and email addresses is not a major obstacle for fraudsters. We appreciate that services have other duties that may help them identify reoffenders, including proactive detection of content and landing pages that have previously been used in scams, but we are wary of platforms only collecting information that is easy for fraudsters to change and then hiding behind the safe harbour provisions of the codes to claim compliance. In our view, Ofcom should make it clear that simply collecting contact information is insufficient. It could achieve this by amending the draft codes, so that services' new duty under FAU/FAS H1.3 (b) (i) reads "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 believe 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. This 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

Ofcom has proposed that a service provider should apply restrictions to advertising accounts found with indicators that there is a material risk that they will post fraudulent advertising. It has also suggested that service providers should apply restrictions as part of the reasonable steps they take to prevent banned advertising account holders returning to the service. Restrictions should involve limited ad spend, limiting the number of users able to encounter paid-for advertisements, limiting the ability to target users from particular groups, restricting the use of certain formats, and reviewing any paid-for ads before they can be posted. Ofcom envisages that providers would place these restrictions in situations where they cannot determine that

the account holder has been previously banned, and so cannot prevent them from advertising altogether. Because these accounts pose a risk of posting fraudulent advertising, Ofcom believes that placing restrictions on them will give additional protections to users.

Which? has seen numerous examples of advertiser accounts which had indicators that there was a material risk that they would post fraudulent advertising being allowed to post by platforms without restrictions. In 2022, we reported on a series of investment ads posted by a company called Tesler. The brand name was already on the FCA watchlist and we could not find any evidence of a real, registered company called Tesler Investments. Moreover, some Tesler ads linked to websites impersonating known brands, including Forbes. In this case, we could not be certain that this Tesler was the same operator that the FCA had previously warned about. Despite the red flags, Meta did not place any restrictions on Tesler's ability to advertise. If Ofcom's proposed measure had been in place, it is likely that services which encountered Tesler adverts would have been obliged to place restrictions on its ability to advertise, which would have given additional protections to users as Ofcom has suggested.

As we have already noted, fraudsters commonly impersonate well-known brands in order to promote fake products or to harvest users' data. We have seen examples of this in relation to Costco and to Aldi in recent years. No restrictions were placed on these ads, despite the fact that their unverified claims to represent major brands could be interpreted as indicators that they were likely to post fraudulent advertising. In fact, the fraudulent Costco advertiser had 300 ads running across Google and YouTube at the same time. Again, had the above measure been in place, the visibility of these ads would likely have been restricted, and so too would have been the harm the ads were able to cause.

We have also seen suspicious ads in video format reappearing time and time again without any proactive steps taken by platforms. We first reported on the Quantum AI scam - a fraudulent cryptocurrency investment scam - in July 2023. We have since reported on the scam in February 2024, November 2024, July 2025, October 2025, and March 2026. The scam frequently uses deepfake videos of celebrities to convince consumers to invest in fraudulent cryptocurrency schemes. Services have frequently removed Quantum AI's videos, only to allow them back onto their platforms after some time has elapsed. If Ofcom's proposed measure had been in place, it is likely that services would have had to take measures against Quantum AI's ads, such as restricting how widely they could be distributed or restricting the use of video in the ads. This would likely have given additional protections to consumers.

Overall, it's clear to see that this proposed measure, if properly implemented and enforced, has the potential to restrict the ability of fraudsters to target consumers at scale. Which? therefore supports this measure.

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

Ofcom has said that providers should conduct repeat checks where providers no longer have confidence that an existing check remains accurate or where there are relevant changes identified on an account. According to Ofcom, repeat checks may be necessary if providers suspect that an account has been subject to account takeover, if the account has changed the type of advertising it posts, if there has been a change in the individual or organisation the advertising account holder is advertising, if an account has become active again after a period of inactivity, or if an account has changed its account name.

Our evidence supports the need for such a measure. In 2024, we reported on a hacking scam on Facebook. Fraudsters would compromise an existing Facebook account and then post attention-grabbing content alongside a link. The aim of the scam was to download malware onto the device of anyone who clicked the links. We've also reported on cases of legitimate WhatsApp business accounts being hacked and used to disseminate scam content. It is clear from these examples that scammers will use account compromise as a tool to target consumers, and tactics may increase as more account-level checks are imposed as a result of the fraudulent advertising codes of practice. Therefore, we feel it is important for services to repeat any checks they carry out on accounts that are exhibiting signs of account takeover.

Similarly, we have seen numerous examples of fraudulent advertisers suddenly changing the name or the nature of the advertising posted in order to run fraudulent campaigns. In July 2024, we reported that scammers had rebranded the same scam profile - a fake car leasing firm - eight times in one year. Despite this constant rebranding, the platform does not seem to have conducted any due diligence on the profile, nor placed any restrictions on its ability to advertise.

In July 2026, we reported on a scam operated by a company called Picadex, which advertised the sale of portable air conditioners but which sold either faulty products or no products at all. Similar to the previous example, we found that the company behind the advertiser profile had changed its name on that profile three times in five years. Based on our investigation, it seems that Picadex posted numerous adverts for portable air conditioners during recent UK heatwaves; however, when we wrote the article in question, we could not see any adverts, suggesting that it rapidly posted numerous ads to take advantage of a specific situation before returning to dormancy. Again, the platform in question does not appear to have conducted any additional checks nor placed any kind of restrictions on this company's ability to advertise.

Finally, in our 2022 report on financial scam ads on Meta platforms, we found that scammers would post their scam adverts from a wide variety of pages, including pages on cooking and current affairs. This was despite the fact that the content was clearly financial in nature, and had nothing whatsoever to do with cooking or current affairs. Despite this disconnect, it appears that Meta did not subject the accounts in question to any additional scrutiny, nor did they place any restrictions on the advertiser's ability to publish ads, though in fairness they did remove ads that Which? had flagged to them.

The above examples illustrate that platforms have a weak track record when it comes to conducting checks on existing accounts that exhibit signs of suspicious behaviour or account takeover. In our view, this fully justifies the need for Ofcom's proposed measure. 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. We therefore support Ofcom's proposal.

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.

Please see above.

3. Preventing fraudulent financial services advertising

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

Ofcom is proposing that providers have a financial services verification policy which sets out the types of permitted financial services advertising, how the provider will find financial services adverts and those posting them, and how the provider will verify that individuals and firms posting financial services ads have the appropriate legal permissions. Providers should publish a summary of this policy and review and update the policy at least once a year. Ofcom considers this to be an "essential step in reducing online fraud, and safeguarding users against one of the highest impact drivers of large-scale financial loss."

Which? strongly supports this proposal, due to the increasing prevalence and widespread harm caused by investment scams. We have been reporting on investment scams for years and in some cases - such as the case of Quantum AI - we have reported on the exact same investment scam across numerous years. In April 2024, we revealed that reports of investment scams on social media trebled between 2019 and 2022, while losses increased more than fivefold, from GBP13 million to GBP75 million. Investment scams can often lead to extremely high losses, on top of the substantial psychological harm caused by scams. Therefore, we believe it is essential that services take measures to prevent investment scams.

We support all of the specific mechanisms that Ofcom has suggested in relation to financial services verification. We want to emphasise in particular 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. We expand on both of those features below.

Our evidence shows that online platforms have a track record of allowing people to advertise financial services products even if those people do not have the requisite authority to do so. In March 2026, we reported on videos promoting the fake trading platform Quantum AI, despite the fact that the advertiser does not have the requisite legal permissions to promote financial services products.

Our evidence also shows that online platforms have not historically prevented individuals on the FCA warning list from advertising. In March 2021, we published an investigation which found that firms were able to advertise on major search engines for weeks after the FCA had issued warnings to avoid them. In December 2021, we reported that an advertiser calling itself 'UK Bonds Investment' was advertising on Facebook, despite the fact that this exact firm had been on the FCA warning list since September 2020. We found adverts being posted by the same advertiser again in April 2024. Which? therefore supports the requirement for services to set out how they will prevent advertisers who are not legally permitted persons or who appear on the FCA warning list from advertising on the service.

Which? has also seen examples of scammers posting financial services content using pages that are not dedicated to financial services. For instance, the Quantum AI scam has in the past presented its adverts as news stories on major current affairs websites, rather than explicitly as financial services ads. Likewise, we have seen examples of scam adverts being disguised as educational courses. Finally, we have seen evidence of pages which are not dedicated to financial services being used to post fraudulent investment ads. This suggests that fraudsters seek to disguise investment ads to avoid scrutiny, meaning platforms must actively seek them out in order to ensure that only FCA-approved organisations are posting investment ads on online platforms. As such, we agree with Ofcom's proposal that a provider's financial services policy must set out how the provider will find financial services investments.

We also agree with Ofcom's provisional assessment that services will need to use proactive technology to detect financial services advertisements prior to them being made available to UK users. As we argued in our 2022 research paper Toward a future without fraud, the sheer scale of the advertising platforms in scope of the fraudulent advertising duties means that using human detection alone is likely to be slow. Our research also found that automated detection models were effective in flagging high risk investment adverts within a dataset that we had collected. We strongly believe, therefore, that it will be possible for services to use proactive technology to identify financial services advertisements. We understand that Ofcom intends to consult on a measure recommending that providers of Category 1 and 2A services use proactive technology to identify financial services investments. We await that consultation with interest.

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. We believe that, should Ofcom's proposed measures in relation to user verification be robustly enforced, it will become more difficult for fraudsters to set up their own fraudulent accounts on advertising platforms. While we were collecting evidence for our response to Ofcom's call for evidence on the third phase of online safety, stakeholders told us that fraudsters would likely pivot to compromising existing verified accounts in such circumstances. We have also heard anecdotally that the onset of age verification requirements for certain services under the OSA has led to a spike in account compromise attempts in relation to those services. Therefore, we think it is important that providers should implement an account security mechanism on all advertising accounts.

We appreciate that Ofcom wishes the measure to be principles-based. We appreciate also that Ofcom does not wish to mandate specific account security mechanisms to enable the codes to evolve along with

technological developments in the account security space. We note that Ofcom states in its summary of the measure that multi-factor authentication is an acceptable account security mechanism. While we agree with this, we believe that MFA via one time passcodes is too susceptible to being compromised and therefore should not be considered sufficient to comply with this measure.

Which? has written extensively about how one time passcodes leave consumers vulnerable to account compromise. In August 2025, we conducted an investigation which found that the use of easily compromised SMS-enabled one time passcodes by some banks may be leaving consumers at increased risk of digital wallet fraud. We found that fraudsters send a phishing message to consumers containing a link that takes them to a fake website where they are prompted to enter their details to complete a transaction. The scammer monitors the website in real time, using the entered information to set up a card on their own digital wallet. Consumers are then sent a one time passcode. The fake website will demand that the consumer enters the one time passcode. When the consumer enters the one time passcode, the scammer is able to add the consumer's card to their own personal digital wallet.

Scammers can also obtain one time passcodes sent over SMS via Sim-swaps. In 2025, Which? reported instances of scammers hijacking phone numbers to steal one time passcodes and compromise online accounts had doubled year-on-year.

It is easy to imagine scammers repeating this trick with advertising accounts. The scammer might contact an account holder, prompting the account holder to enter their details on a fake website, and tricking the account holder into entering a one time passcode which gives the scammer the access they require.

Such an attack would not be possible were the account holder using a different method of authentication, such as app-based authentication. We note that Ofcom refers to the National Cyber Security Centre's 2024 publication, Multi-factor authentication for your corporate online services, in its discussion on ensuring account integrity. In this publication, the NCSC states that "message based methods [of multi-factor authentication] are only likely to be appropriate when no other strengthening method is possible."

We believe it is extremely unlikely that categorised services will not be able to use a stronger method than message based two-factor authentication. Currently, Ofcom's proposed measures FAU/FAS H3 say that platforms' account security mechanisms should reflect current guidance issued by UK government departments, agencies and law enforcement bodies. In our view, this means that use of message-based two-factor authentication is not likely to be an appropriate method unless regulated services can demonstrate that they cannot deploy a stronger method. While we appreciate that Ofcom may not wish to be so prescriptive in the actual codes of practice, we believe that Ofcom should state in its 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?

Please see above.

5. Advertising bans

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

Ofcom has proposed measures FAU H5 and FAS H5: providers should ban advertising account holders that post fraudulent advertisements or fraudulent advertising proxy, and take reasonable steps to prevent them from returning to the service. Which? agrees with this proposal.

Our evidence suggests that measures that fall short of a ban, such as warnings or 'readers' notes' will not be as effective as bans. Our evidence also suggests that fraudsters whose content is removed, but who are not banned, will simply continue to post fraudulent content, thereby harming more consumers. Finally, our evidence suggests that those who are removed from platforms will seek to rejoin under a new account and to

post similar fraudulent content, meaning that bans alone will not suffice; platforms must also have measures in place to prevent fraudsters from returning to the platform.

Which? believes that a punishment for the posting of fraudulent advertising which falls short of a ban is not likely to be as effective as bans. In 2024 we reported on a scam advert on X featuring a video where Martin Lewis supposedly shared financial advice. X did not initially remove the post. Instead, it added a "readers' note" to the post, which stated that: 'This is yet another crypto scam using celebrities.' However, our research has shown that common psychological biases make it difficult for people to detect scams, and that scammers deploy tactics which can impair people's ability to make logical decisions. Therefore, there is a possibility that some people will not believe a 'reader's note' and will engage with the scam content regardless, leading them to experience harm.

Moreover, our research into the Open Display Advertising market shows that there is widespread fraud within that market that is perpetrated by organised criminal groups. As Ofcom notes in Volume 3 of the fraudulent advertising codes consultation, organised groups of this nature are unlikely to be deterred from posting fraudulent advertisements by sanctions such as strikes or account restrictions.

Our evidence also shows that fraudsters who have their content removed but who are not themselves banned from platforms will continue to offend. In 2026, Which? found that sellers on Etsy who had their illegal listings removed but were themselves not banned from the platform simply opened another shop with a slightly altered name and continued to sell illegal products. In 2022, Meta removed suspected fraudulent ads posted by an account called 'UK Bonds Investments' following a prompt by Which?. However, within a few weeks, Which? found an ad which linked to an identical site as the previous fraudulent ad, but which was posting under a different name. In both of the above cases, banning the users instantly after they had posted fraudulent content and taking measures to prevent their return would have reduced the subsequent harm experienced by consumers at the hands of the fraudulent actors in question.

Our evidence also shows that scams will recur even when users are removed. In 2024, Which? reported on a case of scammers impersonating a genuine company in Essex and using its identity to run scam adverts. Once Which? had alerted Meta to the scam, the scammer's profile was briefly taken down. However, the profile soon reappeared under a slightly altered name, and has since rebranded several more times. This highlights the importance of services taking steps to prevent a banned person from creating and using new advertising accounts, as per the draft code.

Our evidence also shows that certain kinds of scam can recur long after the initial content was flagged for removal. In November 2024, Which? reported on an investment scam - Quantum AI - which we discovered in various social media posts and ads on Meta platforms. In March 2026, we found Quantum AI scam content again, once again on Meta platforms. To counter this, firms should use information from previous advertising moderation decisions to identify similarities between the content posted by previously banned users and content posed by new users.

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

No response

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.

No response

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.

In volume 4 of its consultation, Ofcom outlines seven proposed advertising moderation measures both for user-to-user services and search services. The measures are broadly similar, save for the fact that user-to-user services must swiftly take down fraudulent advertisements, while search services must swiftly ensure that individuals are no longer able to encounter fraudulent advertisements.

Ofcom believes that having an effective advertising moderation function is essential for service providers to be able to identify and take swift action in response to fraudulent advertisements on their service. Which? agrees with this. In the following sections, we provide our assessment of each measure.

Having an advertising moderation function to review and assess suspected fraudulent advertisements

Which? agrees with this proposed measure. It is difficult to see how a service provider could comply with its duties under the Act were it not obliged to review and assess suspected fraudulent advertisements.

We agree that providers should have to make a fraudulent advertising judgement when they have reason to suspect that an advert might be fraudulent, or otherwise check the ad against its terms of service or advertising contracts if it suspects the ad might be in breach of those.

We note that volume 4 of the consultation states that providers should not rely solely on user reports to alert them to suspected fraudulent advertisements. We agree with this. Our internal analysis of Ofcom's Online Experiences Tracker has found that less than 40% of people who experienced a scam reported or flagged it. Were platforms to rely solely on user reporting, the majority of fraudulent content would go undetected. Ofcom suggests that platforms should also rely on automated technology and trusted flaggers to detect suspected fraudulent adverts. However, the draft codes of practice for user-to-user services and search services do not state this explicitly. We appreciate that Ofcom has proposed a separate measure on trusted flaggers and will propose a measure on proactive technology, but Which? feels that Ofcom should state clearly in the codes of practice that it is insufficient for services to rely solely on user reporting.

Having an advertising moderation function that allows for swift take down of fraudulent advertisements; having a search advertising moderation function designed to action fraudulent advertisements

These proposed measures require providers to have systems and processes designed to swiftly take down fraudulent advertisements of which they are aware, or for search services, to ensure that users can no longer encounter fraudulent advertisements of which the service is aware. Which? agrees with these proposals and believes that the proposed measures should also require a maximum time period within which ads identified as fraudulent ought to be removed.

These measures are necessary because, in our experience, it is not currently the case that services swiftly take down fraudulent advertisements of which they are aware. As we said in response to the previous question, in November 2023, Which? found that criminals were impersonating a genuine company based in Essex, having stolen its name, company number and other details from Companies House. Which? reported the scam to Meta, but Meta failed to remove the profile. The profile finally disappeared when Which? worked with BBC One's Morning Live to expose it to a wider audience, though it is not clear whether it was Meta or the scammers that removed the profile.

In 2024, a Which? investigation outlined how online marketplaces were failing to protect shoppers using their platforms. Which? deliberately listed products that were illegal to sell in the UK to see whether online marketplaces would be able to detect them. When the marketplaces initially failed to do so, Which? anonymously reported the listings. In some cases, the online marketplaces ignored the anonymous report, and only removed the products when Which? approached them directly to inform them of what had happened. Both of the above examples indicate that, without concrete incentives, platforms will often fail to

remove illegal content, even when it is reported to them. Therefore, we support the inclusion of an obligation for services to remove fraudulent advertisements of which they are aware.

In volume 4 of the consultation, Ofcom states that "we are also not proposing to provide detailed guidance on how quickly service providers should act on identified fraudulent advertisements." This is because Ofcom expects "providers will have systems and processes in place to remove paid-for advertisements they have assessed to be fraudulent as quickly as it is feasible for their service and the paid-for advertisement involved." In both the draft codes for user-to-user services and search services, Ofcom states only that services should take action "swiftly." Which? believes that Ofcom should stipulate a maximum time period during which services must remove fraudulent advertisements of which they are aware. This is because even a short delay in removing a fraudulent advertisement can lead to thousands of additional consumers being exposed to the ad. On 12 March 2025, Financial Times journalist Martin Wolf reported fraudulent adverts to Meta which used deepfakes of him to advertise fraudulent investment products. At this point, the ads had been seen by around 107,000 people. By 13 March that number had increased to 155,000. Which? believes that services should have to remove fraudulent adverts within 24 hours of assessing that the advert is fraudulent. This will help to limit the spread of fraudulent ads and the number of consumers who can encounter them once they have been identified as fraudulent.

Performance targets

Ofcom has proposed that providers should set performance targets for their advertising moderation function, covering at least the time between the service suspecting that users can encounter a potentially fraudulent advertisement and any moderation action, as well as the accuracy of decision making. Providers must effectively measure and monitor their performance against their targets.

Which? believes that, for the purposes of transparency, providers should have to publish a report detailing their targets and their performance against the targets. We know that platforms' internal policies will often prioritise protecting revenues over removing illegal content. For instance, Reuters has reported that Meta's team responsible for vetting questionable advertisers was not allowed to take actions that could cost Meta more than 0.15% of the company's total revenue. Forcing services to publish their targets and their performance against them 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. This would have an overall benefit for UK consumers, since more ambitious targets would lead to better moderation outcomes, whilst reporting requirements would impose minimal costs on platforms.

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.

No response

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.

Ofcom has proposed seven measures in relation to advertising complaints. These are:
Enabling complaints;
Having easy to find, easy to access and easy to use advertising complaints systems and processes;
Appropriate action for advertising complaints about suspected fraudulent advertising;
Appropriate action for advertising complaints which are advertising appeals;
Appropriate action for advertising complaints which are advertising appeals - action following determination;
Exception: manifestly unfounded advertising complaints; and

Dedicated reporting channel for trusted flaggers to report suspected fraudulent advertisements. We do not address all of these measures in our response and have indicated the measures to which we are referring using subheadings below.

Enabling complaints

Ofcom has proposed that service providers should operate systems and processes which enable prospective advertising complainants to make advertising complaints, in a way that will ensure appropriate action is taken in relation to them. Which? agrees with this proposal. There will always be some adverts that are able to evade the other safety mechanisms that Ofcom has proposed, and without a reporting mechanism, these scam ads will continue to remain live and consequently defraud consumers. Enabling complaints is therefore a vital part of protecting users from fraudulent ads.

Having easy to find, easy to access and easy to use advertising complaints systems and processes

Ofcom has proposed that service providers should make advertising complaints systems and processes easy to find, access and use. This means in practice that reporting functions should be clearly accessible, that processes should only include reasonably necessary steps, and that complainants should be able to provide supporting information. Which? supports this proposal.

Our evidence suggests that many consumers are not aware of the fact that they can report scams to platforms, or if they are aware, they do not know how to do it. In our 2024 Victims of Fraud Survey, we found that only 8% of people reported a scam to a website or an app. Of those who did not report a scam to the website or app on which they saw it, 23% did not do so because they did not know that they could, while 20% did not do so because they did not know how. 37% of victims reported finding it difficult to report scams to the online company where the scam took place. This suggests that there is room for improvement in terms of online platform reporting processes. More streamlined reporting processes should result in more scams being reported, which means that those scams will have less chance of defrauding consumers and that services can build more accurate models for detecting scams in future. Both of these outcomes will provide benefits for consumers. Therefore, we support the proposal.

Appropriate action for advertising complaints about suspected fraudulent advertising

Ofcom has proposed that when a service provider receives an advertising complaint about a paid-for advertisement which may be a fraudulent advertisement, it should treat the paid-for advertisement in question as a 'suspected fraudulent advertisement' and review it in accordance with the proposed advertising moderation procedures. Service providers may disregard manifestly unfounded advertising complaints. Which? supports this proposal.

This measure is necessary because, in our experience, services do not always act on advertising complaints. In February 2024, our researchers collected more than 90 examples of potentially fraudulent adverts. Whenever we were confident of something being a scam and wherever in-site reporting tools were available, we reported the adverts. However, it was seldom clear to us whether platforms had taken any action, especially since the majority of platforms did not update us about the outcome of these reports. In 2022, we reported on scam investment ads on Meta platforms operating under the alias UK Income Bonds. Many users reported these ads to Facebook at the time, but the platform did nothing, telling users that the posts did not breach Facebook's community standards. It was only when Which? approached Meta that the ads were taken down. In the same year, we reported on a series of scam ads for diet pills which appeared across numerous services, including Facebook, Bing, Google Search and Twitter (now X). Neither Facebook nor Google responded when we flagged the ads, while Twitter told us that the ads did not violate Twitter's rules. This pattern of behaviour suggests that platforms, left to their own devices, will not presume that content which is flagged to them by users is fraudulent and will lean towards allowing the content to remain live, posing a threat to consumer safety. Therefore, we agree with Ofcom's contention that platforms should treat adverts flagged by users as suspected fraudulent advertisements and should only refuse to take action if

they have a compelling reason to do so. We believe the proposed measure, if properly enforced, should lead to more fraudulent ads being taken down, thereby improving the safety of UK consumers, therefore we support the measure.

Dedicated reporting channels for trusted flaggers to report fraudulent advertisements

Ofcom has proposed that service providers should make a dedicated reporting channel available for submitting reports about suspected fraudulent advertisements if a recommended trusted flagger requests access to one. Which? agrees with this proposal.

As we argued in our response to Ofcom's consultation on protecting people from illegal harms online, Which? believes that trusted flaggers will result in enabling services to build more effective systems that continuously improve over time. However, as we argued during the illegal harms consultation, we believe that the list of trusted flaggers misses organisations that have important data that could be useful for identifying fraud on services. These are the Specified Anti-Fraud Organisations (SAFOs) listed in the Serious Crime Act 2007, which include Cifas, Experian, and the Insurance Fraud Investigators Group. Including these organisations will mean that services can leverage the knowledge and capabilities of organisations that are recognised by the UK Government and have a proven track record in this domain. This would mean more relevant information flowing to services, which should mean more takedowns of fraudulent adverts and consequently better outcomes for consumers. Therefore, Which? recommends that Ofcom expand the list of trusted flaggers to include SAFOs.

We also note that, per Ofcom's report Online Safety in 2025, trusted flaggers have cited poor engagement with a small number of providers under the existing measure in the Illegal Harms Codes of Practice. In order for this measure to be effective, Ofcom must ensure that this poor engagement is addressed.

Ofcom has also proposed that a complaint submitted through a dedicated reporting channel by a trusted flagger, in line with its expertise and related to a specific paid-for advertisement on a service, should amount to a reason to suspect that a paid-for advertisement may be fraudulent and should be reviewed in accordance with their advertising moderation processes. Which? agrees with this proposal. Evidence suggests that, as it stands, platforms are not responding to reports from trusted flaggers with alacrity. In a recent submission to the Treasury Select Committee, the (FCA) provided the average number of days it took for platforms to comply with takedown requests. It noted that Facebook took on average nine days to action a takedown request, and that X told the FCA that it would only take action against posts that it deemed breached its internal policies. Ofcom's proposed duty, if properly enforced, could ensure that platforms act more quickly when they receive requests from trusted flaggers like the FCA, resulting in more takedowns of fraudulent adverts and a higher degree of consumer protection. For this reason, Which? supports Ofcom's proposal.

5. Ad libraries

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

Ofcom is proposing that services should have a library which they make publicly available. The ad library should function reliably and consistently. Services should regularly consult with experts and take account of their suggestions to update and improve the ad library. Ad libraries must contain specific kinds of information about ads (advertising account name, advertiser name, advert content, target audience by demographic, target reach, content keywords used to target users making searches, previous account names, and advert status), and this information must be available for one year after the ad could no longer be encountered by UK users. Services are expected to update the ad library on a daily basis. The ad library must enable keyword and exact phrase searching, a search function that allows users to search for specific accounts, and the use of APIs to allow computer systems to search the library via automated means. Overall, Which? agrees with Ofcom's proposal, although we would welcome some clarifications from Ofcom, as well as some small tweaks to the proposal. At the end of this section, we have also suggested some additional measures

we'd like Ofcom to introduce, as well as evidence supporting the necessity of those measures.

Ad libraries are vital for civil society scrutiny of online platforms, and Which? has used ad libraries on several occasions to highlight the presence of scam adverts on online platforms. In December 2022, Which? conducted research alongside Demos Consulting, which used human and automated analysis to find risky investment adverts at scale in Meta's ad library. In November and December 2023, Which? searched major social media sites - including Meta's ad library - and found Facebook and Instagram hosting multiple copycat adverts impersonating major retailers around the time of the Black Friday sales. In July 2025, our researchers looked at Meta's ad library and found 62 ads claiming to sell weight loss pills using the brand of television programme Dragon's Den. Without access to Meta's ad library, it would be much harder for us to carry out this work and therefore to shine a light on prevalent scams and poor platform practices, as well as to report fraudulent advertising. An inability for us to do either or both of these things would mean more fraudulent advertising being present on services, which would ultimately mean more harm for consumers. In order for us to continue this work and to extend it to more services, it is important that Ofcom mandates that all categorised services maintain a publicly available ad library.

Which? agrees that ad libraries should be publicly available. However, we feel that the current wording of the measures FAU/FAS E1.3 - that ad libraries should be available to "non-users" - is too vague. Ofcom's explanation of the proposed measure states explicitly that "It [the ad library] should be accessible to all who wish to use it, without registering to access." We believe Ofcom should make this explicit in the codes by amending the wording to read "This should be available without the need to register or login to access, including where APIs are used."

Which? agrees that ad libraries should need to function "reliably and consistently." We have experienced issues with Meta's ad library from time to time, including receiving search error messages even though the library says that the system status is "good." We believe that services should have to 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. We recommend that Ofcom adds such a provision into the draft codes.

Which? broadly agrees with the kinds of information that Ofcom has suggested ad libraries contain. We agree that ad libraries should contain the name of the account that posted the ad and the name of the person that the advertising account is registered to. We believe that this should remain the case even for adverts that are banned. Our experience is that, currently, some services redact the name of banned advertisers in their ad libraries. There have been situations where, as a result of this policy, researchers have been unable to state conclusively that fraudulent adverts in an ad library were a match with organisations who appeared on the FCA warning list. Ensuring that the name of the advertiser is always visible would make it easier for researchers to find scam ads and would likely lead to researchers finding more scam ads, which would improve consumer protection against fraudulent ads. We therefore urge Ofcom to clarify that the name of the advertiser should always be visible, even if the ad was taken down or the user banned.
Primary scammers may hide behind third-parties such as marketing agencies and affiliate networks. To effectively combat this, Ofcom must mandate 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.
In August 2026, we reported on a rogue campaign that tricked users into entering card details via a fake verification pop-up, which was then used to trigger unauthorised recurring subscriptions. The ad was placed by a Dubai-based digital marketing agency operating as "Zodiac Technologies DMCC". However, the website being promoted cycled through revolving brand names, contact details and fee structures.
Ad libraries currently display only the immediate account holder or agency name, meaning the true merchant or entity profiting from the fraud often remains hidden. Requiring transparency around the ultimate beneficiary (alongside the registered account holder and marketing agency) would enable researchers and enforcement agencies to link seemingly isolated scam accounts, track rogue affiliate networks and disrupt fraud operations at scale.

We agree that ad libraries should include information on the particular groups of UK users the ad is targeting. As Ofcom notes in Volume 1 of the consultation, there is evidence to suggest that certain kinds of scam (e.g. investment scams for pensions or crypto investment scams) are targeted at specific demographics. We believe that ad libraries should allow users to review which groups an advert is targeting based on all of the targeting variables offered by the platform. For example, if an advert is targeted at an individual because they have expressed an interest in a certain topic, we think that should be visible in the ad library. We believe that Ofcom should amend 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.

Currently the draft codes state that ad libraries should include information about the number of UK users the relevant ad is targeting or the number of UK users who have encountered the ad. Which? believes that the library should have to include information on both of these metrics, as both of them provide different insights and are therefore useful for researchers and campaigners. Which? also believes that the number should 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. Finally, Which? believes that ad libraries should include 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.

Which? agrees that data on the ad library should be available for a year after the ad can no longer be encountered. We would like to see 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). The reason should be specific; for example, knowing that an ad was taken down because it was advertising a financial services product without the required authorisation is useful, whereas knowing that an ad was taken down because it violated the platforms' policy is less useful. This will help civil society organisations, Ofcom, and other regulators to understand which fraud offences are easier for platforms to infer when conducting advertising moderation. This is useful information in terms of thinking about any changes to the Act in the future, or whether Ofcom needs to revise its Illegal Content Judgement Guidance.

We also agree that data on the ad library should be updated daily. We believe that this data should include all adverts uploaded within a given 24-hour period, even where these have been deleted before the end of that period. This would ensure that the ad library captures advertising campaigns that only last for a number of hours.

While we agree that there should be keyword and exact search phrase options for ads, we believe that there should be additional search criteria to allow for users to make granular searches. These additional criteria should include: live/closed ads; the target geography of the ad; the number of users reached; and the advertiser. Our experience of the current search functions of ad libraries is that they are subpar. By enabling more granularity in search, ad libraries will become easier to use, increasing transparency and thereby consumer protection from fraudulent ads.

We agree that ad libraries should enable users to search for relevant ads posted by specific accounts. We believe that each advertiser's account should include a search bar allowing users to search for specific ads.

We agree that ad libraries should enable the use of an API to provide a standardised way to allow computer systems to search the ad library and provide enhanced interactivity. This access should not be constrained. Any approval process should be simple and approvals should be granted as quickly as possible. Access should be provided on a frictionless, self-service basis. Where technical measures like API keys are required to manage system load, these must be issued automatically upon request, without any discretionary gating or approval process that could restrict access for researchers. This will make it easier for researchers to access

ad libraries, improving the overall transparency of the system.

Ofcom argues in the draft codes that links can be indicators of fraudulent advertising when they:
do not take the user where they purport to; or
lead to fake websites or websites that coerce the user to perform an action.

Our evidence supports this assertion. In June 2026, we reported on a wave of social media scams that featured fake influencers selling suspicious products. In these cases, the websites to which the ads redirected users were key pieces of evidence that the ads themselves were fraudulent, since each website contained typical signs of being scams. The content itself, at least at first glance, was relatively innocuous. If we had found such ads in an ad library and the click-through links had not been available, it would have been more difficult for us to conclude that the ads were likely fraudulent. As such, we believe 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.

The same scam can often recur over several years. For example, we first reported on the scam advertiser calling itself 'UK Bonds Investment' in January 2022. We reported on the same fraudulent advertiser again in April 2024, though at this time it was calling itself 'UK Income Bonds.' In this case, the advertiser had been on the FCA warning list since September 2020. Similarly, the FCA warning list contains numerous examples of scam companies - such as Coverfast/Temprdrive - which have been able to run scam ads over a number of years by repeatedly changing its name and details. Currently, Ofcom only recommends that information on an ad library be stored for 12 months after the advert is no longer live on a service. This means that, if a researcher were to find a long-running scam such as the UK Bonds Investment/UK Income Bonds scam, they would not have access to the full archive of previous scam ads, which might lead them to underestimate the scam's longevity and overall prevalence. Which? believes that it is useful for researchers and campaigners to be able to show that the same firms are able to pop up and post scam ads time and again, as this will lead to better understanding of scams and, ultimately, better consumer protection outcomes. Therefore, we recommend that the draft codes be updated to stipulate that adverts should be stored for at least five years after they stopped being live on a service.

Additional comments

Ads can display trusted domains but execute redirects to trap victims, a tactic used in a Tesco scam we reported in May 2024. If the displayed link differs from the final destination, Ofcom should require ad libraries to log the full list of redirects and the final user landing page.

Scammers also exploit platform checks by abusing verified advertiser status to impersonate legitimate businesses. In February 2024, we uncovered fake Lyca Mobile ads run by an account that Google had verified under "Vodafone". Clicking the ad redirected users to a copycat site that stole payment details. Platforms confirm that a company exists, but fail to verify whether an account has any authorisation to advertise on behalf of that brand. Ofcom should mandate that ad libraries explicitly show whether an advertiser holds verified brand authorisation for the trademarks they target.

A Which? investigation into click-to-call scam ads in December 2025 highlights a similar gap in platform transparency. Here, scammers bypass traditional landing pages entirely, inviting users to call fake call centres by impersonating trusted brands and targeting search engine queries like "Three mobile help" or "call Three". Ofcom should include specific provisions for click-to-call ads, requiring ad libraries to disclose targeted search keywords, attached phone numbers, and verified brand authorisation status.

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.

See above.

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?

No response

Additional questions

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

No response

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

No response

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

Ofcom is proposing to publish a Fraudulent Advertising Judgements Annex, which adapts the existing guidance for illegal content to take account of paid-for advertising, including targeted offence-specific updates and cross-cutting guidance on reasonably available information. Ofcom has also proposed consequential updates to the Illegal Content Judgement Guidance (ICJG) to ensure consistency with the new annex and wider regulatory developments.

Ofcom is proposing to add two examples to the ICJG's list of examples of common false representations. These examples are intended to capture instances of advertisements being used to promote medication which is sold without prescription, controlled drugs, and weapons which cannot be bought or sold legally in the UK. Which? supports this proposal. In June 2026, we reported on deepfake adverts which led to a website selling fake weight-loss patches. In June 2025, we reported on numerous adverts marketing a bee venom cream which the advertiser falsely claimed was developed by the Medical and Health Care products Regulatory Agency. These examples demonstrate the false claims about medication are commonplace on services. Amending the ICJG in the way suggested by Ofcom should make it easier for services to identify these adverts as fraudulent and therefore to remove more of them, making consumers safer overall.

Ofcom is proposing to add some additional 'red flag indicators' to the existing list of examples of fraud by false representation contained within the ICJG. These additional red flags are: use of a username or account name which is similar to the username or account name of a brand, company, or public figure; and use of the brand identity or likeness of a person, where characteristics of the account submitting the advertisement are inconsistent with the known characteristics of the brand or person concerned. Which? wholeheartedly supports these additions. In October 2025, Which? reported on a number of scam videos featuring deepfakes of Martin Lewis promoting a fraudulent investment scheme called Quantum AI. Martin Lewis has repeatedly stated publicly that he does not give out investment advice. In May 2025, Which? reported on a scam where fraudsters were able to impersonate Costco's website and appear above the genuine store in the sponsored search results on Google. In both cases, under Ofcom's revised guidance the ads in question would contain red flags and would likely warrant moderation by the services on which they were published, which could result in similar ads being taken down in future, making consumers safer as a result.

Ofcom is also proposing to add the following red flag as an example of potential fraud by false representation: "The advertising account submitting the advertisement shares identifiable characteristics with an advertising account that has already been identified as having posted a fraudulent advertisement." Which? supports this decision. In January 2022, we reported on an investment scam run by an organisation calling itself 'UK Bonds Investment'. We found ads that led to an identical website across numerous accounts with broadly similar names, including UK Bonds Trust and UK Income Bonds. Meta took the adverts down

when Which? reported them, but similar adverts leading to an identical website soon emerged weeks later. Under Ofcom's revised guidance, service providers would likely have to moderate any ad which is similar to an ad posted by an account which had previously posted fraudulent content. This could result in fewer copycat fraudulent ads being posted, increasing the safety of UK consumers overall.

Ofcom is proposing to change the current red flag indicator for fraud by false representation from claims that an "emergency has arisen" to claims that "an opportunity has arisen, and that quick action is required to benefit from it." Which? supports this decision. Our March 2023 report Toward a future without fraud demonstrated that using language that suggests an opportunity is time critical to create a sense of urgency is one of the main ways in which investment ads mislead consumers. Ofcom's proposed modification should mean that more such ads are prioritised for review and removed by moderators, thereby reducing consumers' overall exposure to such fraudulent advertisements.

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

Ofcom considers that information about the destination of an advertisement (including landing pages with a single interaction and other linked webpages) may constitute relevant and reasonably available information. It is proposing to add outputs from URL-scanning tools and services to the Fraudulent Advertising Judgements Annexe's list of 'reasonably available information' for fraud by false representation and misleading statements and impressions about investments.

Which? supports this decision. In April 2023, we reported on fraudulent advertisements in Google Search results. Scammers had paid for their adverts to be at the top of the search page and the adverts stated the URL of a legitimate retailer who the fraudster was impersonating. However, when consumers clicked on the link in question, they were taken to a different website offering rewards in exchange for consumers providing their personal data. Had the service deployed URL scanning technology on the ad, they would have seen that the destination URL embedded in the ad did not match the brand name of the company mentioned in the ad, and they might have further reviewed and ultimately taken down the ad, thereby preventing consumers from interacting with it.