2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

RESPONSE TO DCMS' CALL FOR EVIDENCE ON ONLINE ADVERTISING

Which? welcomes DCMS's Online Advertising Call for Evidence. Which?'s mission is to tackle consumer detriment by making individuals as powerful as the organisations they have to deal with in their daily lives. When it comes to global online advertising platforms, there is clear asymmetry between platforms and consumers. We therefore welcome the government's work in this important area. Our own work on this is continuing to evolve and we would value ongoing engagement with DCMS as our respective thinking develops.

In your Call for Evidence, you set out the government's overarching aim to:

- ensure standards about the placement and content of advertising can be effectively applied and enforced online so that consumers have limited exposure to harmful or misleading advertising;
- promote a competitive and fair online advertising market for businesses so that all businesses can compete on merit; and
- drive transparent and ethical targeting practices for advertising online so that consumers are informed, empowered and can have trust in online advertising.

We note that the call for evidence is focused on the first point above. However, we are also involved in the CMA's market study into online platforms and digital advertising (second point), so we have included an overview of our current position on that as part of this response for your information. Our full response to the CMA's online platforms and digital advertising market study interim report is also attached for completeness.

In relation to the placement and content of advertising, our work and the evidence we have provided particularly relates to fake and fraudulent ads that lead to consumers being misled, scammed or defrauded. We call this 'fake and fraudulent content that enables scams'. We believe this is a key issue for consumers and an area of harm that is currently falling through regulatory gaps. We have therefore focused our response on this issue, its contribution to the scams landscape, and its link to the work on Online Harms regulation.

We also note that fake and fraudulent content online and on social media platforms has been a recent focus in light of the increasing number of coronavirus-related scams we are seeing. Our work in this area is in early stages and we are now starting to gather evidence of how scammers are seeking to profit from the pandemic.

Benefits and challenges of online advertising

The issue: Fraudulent ads as an enabler of scams

Consumers are exposed to harm from online advertising content through exposure to fake and fraudulent ads that enable scams. Specifically, we mean that online advertising is providing an opportunity for fraudsters to intentionally mislead consumers in order to illegally gain money from them, or illegally gain personal information that can provide further opportunities to defraud the victim.

We believe that a lack of regulation around the placement of ads on social media and other online platforms is causing UK consumers to lose millions of pounds to scammers each year. This is on the rise, and ads on social media platforms and search engine results are becoming a key enabler of these scams. Social media and other online platforms are enabling scammers to reach innocent internet users and defraud them[1], which can result in substantial financial loss for victims. Online advertising is one method that scammers use to reach their victims and action is urgently required to address this.

The recent fraud report published by UK Finance sets out that it is not possible to place specific monetary values on particular tactics criminals use (such as fraudulent advertising). However, intelligence reported to UK Finance indicates the key drivers behind the reported figures. UK Finance goes on to say:

> *The increased use by customers and businesses of online services for many different aspects of day to day life is leading criminals to increasingly focus their efforts on defrauding people through online fraud and scams. For example, in 2019 there was an increase in investment scams as criminals turned to online platforms to try to defraud victims of large sums of money. Previously criminals have typically used cold calling to target victims through investment and pension scams. However, criminals have increasingly moved online and the nature of the frauds has become ever more sophisticated.*[2]

According to the UK Finance report, investment fraud is rising with a 90% increase in value lost (£95.4m) and a 101% increase in volume (6,789 cases reported) in 2019. Furthermore, FCA analysis suggests that the rise in investment fraud is being driven in part by criminals targeting consumers online, for example through adverts on search engines or social media channels.[3]

Unauthorised financial fraud losses across payment cards, remote banking and cheques totalled £824.8 million in 2019, and in addition to this there were 122,437 reported incidents of Authorised Push Payment (APP) scams with gross losses of £455.8 million.[4] These huge figures represent significant emotional as well as financial impact on consumers. While we cannot identify how much of these total fraud losses came about from online advertising, the evidence above suggests that the use of online advertising in fraud is increasing. If this makes up even a small percentage of all fraud and scams, it would still account for significant consumer losses. We believe this could be avoided if stronger measures were

[1] For example, UK Finance has noted an increase in investment scams and that scammers are increasingly using social media to reach victims by advertising fake investments.
[2] UK Finance, "Fraud The The Facts 2020", p.7: https://www.ukfinance.org.uk/system/files/Fraud-The-Facts-2020-FINAL-ONLINE-18-March.pdf
[3] Ibid., p.50
[4] Ibid., p.7

taken in relation to fake and fraudulent ads that appear online on social media and in search engine results.

It is currently far too easy for scammers to use online advertising to place misleading, fake and fraudulent ads on social media platforms and websites to reach and defraud consumers. While most online platforms say that they have measures in place to prevent fraudulent content, the number of cases reported into Which? suggests that these are not working effectively to prevent scammers from using online ads to defraud consumers. We also know from our own investigation that fake ads can easily slip through the checks that online platforms carry out, as we highlight in our response below.

Given the potential for harm, it is essential that standards about the placement and content of advertising online, and particularly on social media, are updated to protect consumers from exposure to fake and fraudulent ads. Similarly, we think the online and social media platforms that authorise the publication of these ads need to take more responsibility in screening out those that are fake and fraudulent, which we discuss in more detail below.

Evidence of fake and fraudulent ads

Robust, quantitative evidence on the scale of harm from fake and fraudulent ads is currently lacking, but we believe there is sufficient evidence and examples of this practice happening to justify DCMS taking action in this area. The box below provides some examples of fake and fraudulent online ads, most of which have been reported into Which? over the last year. We know that there are many more out there and considerable numbers of consumers will be exposed to these. In addition, we will be carrying out further research in the near future, which will help us better understand how these fake and fraudulent ads affect consumers. We would be happy to discuss this research with you in more detail.

Examples of fake and fraudulent ads that consumers are exposed to online

Celebrity endorsement investment scams

We have seen examples of fraudsters running fake investment opportunities often using ads on social media to promote "get rich quick" online trading platforms. These ads frequently use fake celebrity endorsements and link to professional-looking websites where consumers are persuaded to invest.[5] Last year, Which? published one case of a woman who saw a Facebook ad for an investment opportunity involving bitcoin, which referenced support from a Dragon's Den episode.[6] This had previously hit the news as a scam and yet the ad was still on Facebook and unfortunately the woman had not seen the news about this scam. The woman authorised a debit card payment of £300, but the scammers then took another £8,500 from her debit card through four further transactions. It took seven months to get the money back from her bank.

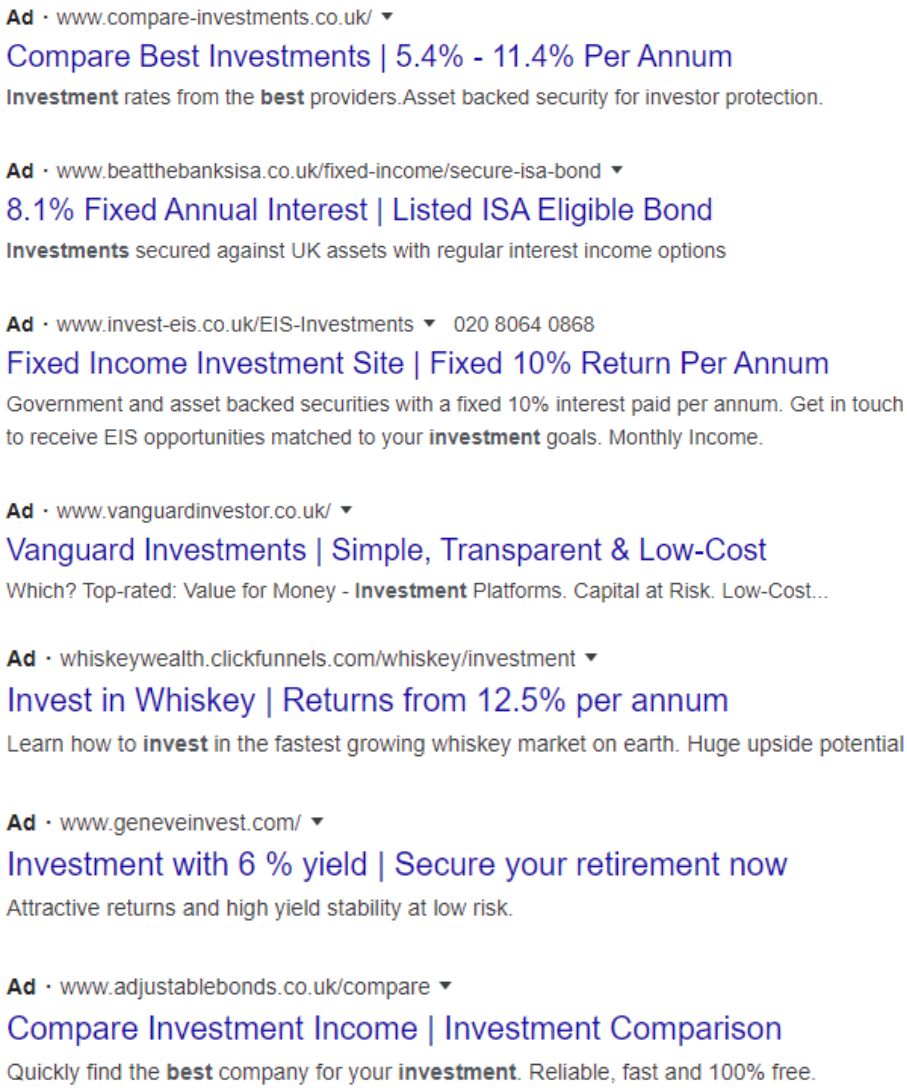
[5] Action Fraud (2019), "Over £27 million reported lost to crypto and forex investment scams": https://www.actionfraud.police.uk/news/over-27-million-reported-lost-to-crypto-and-forex-investment-scams

[6] Which? Consumer Rights (2019), "Renewed warnings about Bitcoin investment scams with fake celebrity endorsements":https://www.which.co.uk/news/2019/03/renewed-warnings-about-bitcoin-investment-scams-with-fake-celebrity-endorsements/

Other investment ads on Google searches

There are around 18,000 internet searches for the term 'best investments' every month in the UK[7], but scammers as well as legitimate companies are paying for online ads and even paying to be among the first search results a consumer will see. According to the latest figures from UK Finance, 3,385 investment scams were reported in 2018, from which victims lost a combined £50.1m, however only £3.9m was recovered.

The images below are screen shots from a Google search for 'best investments'. Worryingly, only two of the advertised companies below were on the FCA register and many offer fixed high returns. We cannot confirm at this stage whether these are definitely scams, but it is certainly dubious practice and it is concerning that consumers are being exposed to these (whether outright scams or high-risk investments without warnings) via a simple online search. It is important to note that while the below examples are from a Google search, we are aware of other platforms, such as Facebook and Twitter, hosting similar ads.



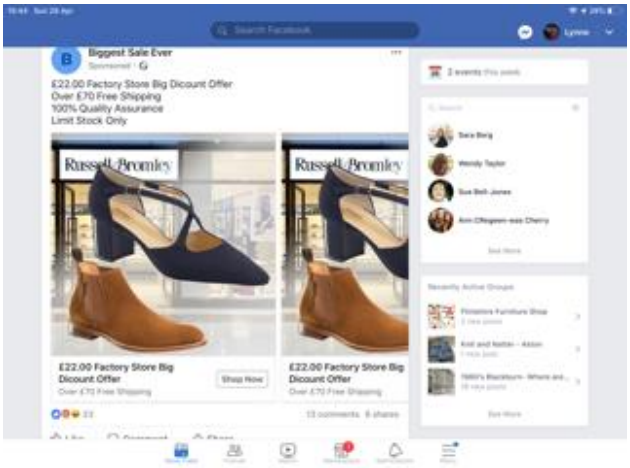
Fake helplines advertised on Google

[7] According to a search using keyword analytic software, SEMrush, in March 2020.

Which? recently published a news article warning consumers about fake helplines that are appearing in paid-for online ads purchased by fraudsters.[8] The article looks at the example of a fake Revolut helpline being advertised on Google and causing consumers to make direct contact with criminals. Unfortunately, Google was unable to tell Which? how long the ad had been online, which company had taken it out or which search terms the ad was targeting. Scammers are paying to advertise these 'helplines' and Google is making money from them.

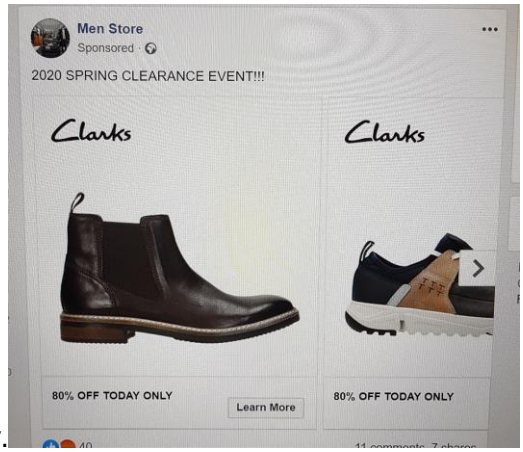
Fake/non-existent products

Which? has seen cases of people clicking on ads for well-known and trustworthy British brands (e.g. Russell & Bromley and Clarks) but later finding out that the transaction has actually been processed in a different currency and the goods never arrive, or the wrong goods arrive. In the examples below, fake Russell & Bromley ads appeared on Facebook and Instagram. When consumers made purchases from the website, they later found that the transaction had been processed in Chinese Yuan, rather than British Pounds, and then the goods never arrived.



We have also received several reports from consumers that have fallen for fake ads for Clarks shoes on Facebook. Two screenshots are provided below as examples. In this scam, consumers think they are ordering Clarks shoes, but then find they have been charged £5 to convert pounds to dollars and later receive a fake designer scarf rather than the shoes they ordered. This appears to be carried out by a Chinese company. Consumers are particularly concerned that they have then unwittingly given their credit card and personal details to this foreign

[8] Which? (2020), "Check your account: fake Revolut helpline advert targeted victims via Google": https://www.which.co.uk/news/2020/03/check-your-account-fake-revolut-helpline-advert-targeted-victims-via-google/

company. 

Fake holiday accommodation

Which? provides advice on spotting holiday scams, as we know that scammers use the popularity of sites like Airbnb and Holiday Lettings to make money by tricking people into booking fake holiday listings. In April 2018, Action Fraud published that losses from holiday fraud in 2017 totalled £6.7 million from 4,700 reported incidents. Action Fraud says that "fraudsters are making full use of the internet to con holidaymakers by setting up fake websites, hacking into legitimate accounts and posting fake adverts on websites and social media".[9]

The existing system of oversight and regulation

Gaps in regulation and advertising policies

We see fake and fraudulent online ads as falling into regulatory gaps and we are disappointed that fraudulent content and scams have been left out of scope of the Online Harms regulations. Online platforms' current terms of service and advertising policies are clearly not working to prevent fraudulent ads appearing online. When Which? reports fraudulent ads and content to online platforms, we are frequently told that they do not tolerate fraud. Unfortunately, that is clearly not enough to protect consumers from fraudulent ads and content.

Which? also believes the advertising policies of online platforms may not be enough to prevent fake ads being placed on them. For example, in June 2019, we published an investigation that looked at how straightforward it is to place fake ads on Facebook.[10] For this investigation, we created a fake ad for a Tesco promotion on a business profile on Facebook, which linked to a website created using a free online website creator. The fake ad stayed up for around a day, convincing some Facebook users to visit the fake website we

[9] Action Fraud (2018), "Action Fraud reports show £6.7 million lost to holiday booking fraud": https://www.actionfraud.police.uk/news/action-fraud-reports-show-6-7-million-lost-to-holiday-booking-fraud
[10] Which? (2019), "How our fake 'scam' ad breezed through Facebook's approval process": https://www.which.co.uk/news/2019/06/how-our-fake-scam-ad-breezed-through-facebooks-approvals-process/

had created, before it was 'flagged for policy violations'. When we asked Facebook to explain its ad review process, it told us that "there's a proactive review every time someone submits an ad … with artificial intelligence and human review". Its terms and conditions also state that ads may not be approved if the landing page content isn't fully functional. Our fake ad obviously got past this monitoring process.

Voluntary initiatives will not be effective

We are concerned that voluntary standards (like the Internet Advertising Bureau's Gold Standard and Better Ad Standards) are falling short and are not effective at sufficiently regulating good practice to protect consumers from fake and fraudulent ads. While these standards may be effective in incentivising some businesses to improve the standards of their advertising, such voluntary initiatives will never be effective in stopping scammers. Scammers will continue to use online advertising as a means of reaching their victims as long as it remains a viable option for them, and right now there are few barriers to prevent the publishing of fraudulent ads online. We therefore believe further action is required to prevent fake and fraudulent ads appearing in the first place.

Action we want to see

Given the lack of effective measures for preventing fake and fraudulent ads appearing online, we are disappointed that the upcoming Online Harms regulations will not be addressing the issues of fraudulent content and advertising on online platforms. We understand that the regulations will place a statutory duty of care on online platforms to self-regulate certain content (such as terrorist and child sex abuse content), which will involve establishing processes and practices to monitor, screen, takedown and prevent such content, but that such a duty will not extend to other forms of harmful online content. We believe this is a crucial missed opportunity and that those same processes should be extended to other types of content, such as fraudulent content or fake ads, to protect consumers from a wider range of online harms.

As we have said in a previous submission to DCMS on Online Harms[11], it would be effective to bring these other harms under the duty of care in the Online Harms proposals. This would then incentivise online platforms to further scrutinise the ads before they are published on their websites to help them meet the duty of care. Additionally, Facebook has committed to introducing a scam reporting tool for ads on its website in the UK. We would like to see other platforms and search engines encouraged and incentivised to do the same, on top of measures to prevent fake and fraudulent ads in the first place.

Further action

Beyond consumers being exposed to harm from fake and fraudulent online ads, we are also concerned that there is no route to redress that consumers can take when they have fallen victim to these scam ads. If a consumer loses money having clicked on a fraudulent ad, they may have some route to getting their money back depending on their payment method, but

[11] Further submission to our original response to the Online Harms White Paper: "Inclusion of consumer harms in the Online Harms White Paper proposals", submitted to DCMS on 15 November 2019.

this must be sought from banks and credit card companies rather than from the company that exposed the consumer to the scam. However, for those who have fallen victim to scam ads and unwittingly shared their personal information with scammers, there is no route to redress and they are likely to be placed on 'suckers lists' that will mean they are more likely to be targeted by scammers in the future. We believe one solution to consumers being unable to seek redress in such cases is for the Government to instate article 80(2) in GDPR when it reviews the inclusion of the clause later this year.

Broader digital advertising landscape

As explained in our response to the CMA's online platforms and digital advertising market study interim report, we agree with the Furman Review about the need to complement existing ex-post antitrust tools with pro-competitive regulatory rules to govern the behaviour of firms that enjoy a position of market power. Ex-ante rules and guidance that provide clarity over what represents acceptable behaviour when interacting with consumers and competitors will help to prevent and address harms to consumers and competition. We also support introducing remedies to improve consumers' control over their data. In particular, the proposal that all platforms be required to give consumers an option to use their services without requiring in return the use of consumers' data for personalised advertising (or any type of targeting outside the core service). We attach our full response to the CMA's interim report describing in more detail our position on those areas.

Finally, we welcome the government's announcement in the Budget to set up a cross-regulator digital market taskforce to complement the insights and recommendations of the CMA's market study to provide the government with the advice needed to implement a pro-competitive regime for digital markets.

About Which?

Which? is the largest independent consumer organisation in the UK with more than 1.3 million members and supporters. We operate as an a-political, social enterprise working for all consumers and funded solely by our commercial ventures. We receive no government money, public donations, or other fundraising income. Which? empowers consumers to make informed decisions and campaigns to make people's lives fairer, simpler and safer.

For further information please contact Stephanie Borthwick, Senior Policy Adviser, Which? at stephanie.borthwick@which.co.uk.

31 March 2020