

Written evidence submitted by Which? (COR0144)

Which? is the largest consumer organisation in the UK with more than 1.3 million members and supporters. We operate as an independent, apolitical, social enterprise working for all consumers. We are funded solely by our commercial ventures and receive no government money, public donations, or other fundraising income. Which?'s mission is to make individuals as powerful as the organisations they have to deal with in their daily lives, by empowering them to make informed decisions and by campaigning to make people's lives fairer, simpler and safer.

Online platforms and marketplaces are now a regular part of everyday life for most people. While there has been rapid change in the way people interact with services and products online, regulations have not kept pace with technological developments, leaving growing numbers of consumers increasingly exposed to numerous online harms.

We therefore welcomed the Online Harms White Paper as a positive step toward much-needed regulation of online platforms. However, Which? has previously expressed concerns about a number of areas not covered by the current proposals where users online are increasingly suffering serious harm, including fake reviews and buying unsafe products.

Online developments during the Covid-19 crisis

1. Recently, we have seen the rise, and in some cases emergence, of a number of online consumer harms as a result of the coronavirus pandemic. This is of particular concern at a time when people are potentially more reliant on going online to access products and services, as a result of the closure of many physical shops and businesses. There are also more people who are more vulnerable, as is the case during times of crisis.

2. The main online harms that Which? is aware of that are directly related to the current pandemic include people losing significant sums of money to sophisticated coronavirus-related **scams and online fraud, misinformation about 5G** infrastructure and widespread examples of **price gouging** on some of the biggest online marketplaces.

3. Which? echoes the Minister for Digital and Culture's comments to the Home Affairs Select Committee on 13 May that all users should be safe when online and that building consumer trust in online platforms would empower users. To support these ambitions, the Government must urgently outline further plans to tackle these harms and to make online platforms more responsible for poor practice and criminal activity on their sites.

Specifically, Which? is calling for online scams and fraud to be brought into scope of the Online Harms White Paper.

4. Online platforms and marketplaces should have greater responsibility to prevent fraudulent, illegitimate and illegal content from appearing on their sites. As well as quick action to remove harmful content when reported, there should be strong incentives for sites to develop systems to prevent such content appearing at all. This preventative action will be more effective in protecting consumers from these harms.

Scams and online fraud

The nature of the problem during the Covid-19 period

5. Which? receives many reports about scams from consumers, but in recent weeks there has been a noticeable shift in the focus of these scams as a result of the coronavirus crisis. While many of the scams remain the same in terms of the sophisticated techniques and tricks used by scammers, increasingly coronavirus is being used as the "hook" to draw in unsuspecting consumers. This has

occurred over a wide range of scams, including those that take place via phone calls (vishing), SMS text messages (smishing), phishing emails and online platforms. Examples of each are included below.

6. Scammers are quick to adapt so they can profit off new situations and public crises. We have seen examples of this before coronavirus. For example, directly following the collapse of Thomas Cook in September 2019, Which? was made aware of scammers trying to exploit worried customers by setting up websites claiming to offer refund services, posing as “Thomas Cook refund agents” in an effort to secure people’s credit card details and sending out text messages purporting to be from banks.

7. We know that scammers are using the coronavirus crisis as an opportunity to scam consumers, as the current situation increases consumers’ vulnerability to scams due to profound changes to people’s lifestyles. Vulnerability should not be limited to static characteristics like disability or age, but should include temporary circumstances, such as bereavement or loneliness, that can make people more susceptible to scams. Current changes to people’s lifestyles may increase their exposure to scams and make it more difficult for people to recognise them. For example, higher levels of stress due to lockdown and, for some, changes in employment, childcare or homeschooling mean that people are likely to be more reliant on online services, distracted, and less vigilant when it comes to spotting a scam. Financial hardship and therefore searching for better deals online can also increase people’s susceptibility to attractive, fraudulent offers. Similarly, as people spend more time in their homes, they are more likely to pick up phone calls, including potential vishing scam phone calls.

8. Investment scams, in particular, appear to be on the rise. The coronavirus crisis is having a profound effect on economic markets, with many people now looking for new investment opportunities and therefore at increased risk of falling for fake investments. While the FCA and several banks have published warnings about coronavirus investment scams, more needs to be done to reduce consumers’ exposure to these scams, rather than relying on consumers to identify these scams to protect themselves. This could include search engines and online platforms taking steps to prevent the publishing of fake investment ads, and domain registries working with authorities and responding quickly to reports, taking down fraudulent phishing domains when they are identified.

Examples of coronavirus-related scams

9. Since the start of the coronavirus crisis, Which? has warned people about a potential increase in scam calls, texts and emails. Such calls could follow typical patterns of callers claiming to be authority figures, including the police, HMRC or your bank, and involve requests to transfer money, hand over sensitive account login information or PIN codes. Vishing scams involving subscription accounts are particularly popular as subscription services are now more in-demand.

10. “Smishing” or scam text messages have also evolved in the current crisis. One example involved a bogus text message claiming to be from the UK Government saying the recipient had been fined for going outside too many times in a day during lockdown, that their movements have been monitored through their phone and they must pay a fine or face a more severe penalty. Many examples of smishing scams include a link for people to follow where consumers will be asked to make a payment or share personal information.

11. There have also been many examples of phishing emails that are directly linked to coronavirus and lockdown. For example, the Department for Education issued warnings about a scam email regarding free school meals which was designed to steal bank details. Other attempts to trick

consumers into giving away personal and bank details in return for the promise of a council tax refund due to the pandemic¹.

12. We continue to see examples of fake supermarket shopping vouchers, which trick people into sharing their personal information with scammers. We have also heard of “fun” coronavirus quizzes being shared on social media that look like they are testing a person’s knowledge of the pandemic, but in reality are gathering personal information that could be used to later defraud them.

Steps that could be taken to mitigate these concerns

- Online and social media platforms must do more to identify and remove fraudulent content that enables scams and to prevent it from appearing on their platforms in the first place.
- Businesses should be encouraged to sign up to existing initiatives such as Ofcom’s Do Not Originate (DNO) scheme, which will help in the fight against vishing scams.
- Widespread adoption of the Mobile Ecosystem Forum’s (MEF) *SMS SenderID Protection Registry*.
- All organisations and businesses should ensure legitimate messages avoid the use of hyperlinks and embedded phone numbers, which are commonly used by scammers.
- Organisations should try to avoid using SMS in coronavirus-related communications, as it is not a secure form of communication.

The effectiveness of current Government Online Harms proposals to address issues

13. We understand that current proposals will place a statutory duty of care on online platforms to regulate certain content (such as terrorist and CSEA 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 strongly believe the current scope of the future online harms regulations and codes of practice are too narrow.

14. This is a crucial missed opportunity to extend those same processes to other types of content, such as fraudulent and scam content, to protect consumers from a wider range of online harms.

Online scams and fraud should be brought within scope of the online harms regulations.

Online platforms and marketplaces should be made more responsible for preventing fraudulent, illegitimate and illegal content from appearing on their site, as well as for quick action to remove harmful content when it is reported.

Fake, fraudulent and misleading online advertising

The nature of the problem during the Covid-19 period

15. It is currently far too easy to use online advertising to place misleading, fake and fraudulent ads on social media platforms and websites. Scammers and those willing to profit from the coronavirus crisis therefore have an easy route to reach and defraud consumers. While most online platforms say that they have measures in place to prevent fraudulent content, these are not working effectively to prevent scammers from using online ads to defraud people. A recent Which? investigation² found that fake ads can easily slip through the checks that online platforms carry out.

¹ <https://conversation.which.co.uk/money/council-tax-reduction-scam-phishing-email-warning/>

² 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/>

16. The Medicines and Healthcare Products Regulatory Agency (MHRA) has also published warnings about fake COVID-19 cures and treatments being sold online. In addition, there have been cases of victims losing money when purchasing personal protective equipment (PPE) or self-testing kits online from fraudulent websites where products simply do not exist.

17. There are also coronavirus-related ads which include misleading or incorrect information. For example, we were made aware of an Instagram advert for a face mask which stated that "it is now essential to wear an anti-pollution mask", despite official Public Health England guidance at the time stating that it did "not recommend the use of face masks as a means of protection from coronavirus".

18. The fact that these dodgy, non-existent and/or misleading products can be advertised online and quickly reach so many consumers is concerning. Given the financial benefits from ad revenues, online platforms must be more efficient and effective in their efforts to take down fake ads hosted on their sites, also taking stronger action to prevent fake ads being published in the first place.

Steps that could be taken to mitigate these concerns

19. It is essential that standards regarding the placement and content of advertising online, particularly on social media, are updated to protect consumers from exposure to fake and fraudulent ads. Similarly, 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, taking them down quickly when they slip through.

20. Given the lack of effective measures for preventing fake and fraudulent ads appearing online, we strongly believe fraudulent content and advertising on online platforms should be brought within scope of the duty of care in the Online Harms proposals. As with scams and fraud, the processes that platforms will be expected to establish under the duty of care should extend to a wider range of online harms, including fake and fraudulent ads. This would incentivise online platforms to further scrutinise ads before they are published on their sites, in order for them to meet the duty of care.

21. Additionally, Facebook has committed to introducing a scam reporting tool for ads on its UK site. We would like to see other platforms and search engines introducing tools to allow consumers to report fraudulent ads.

The effectiveness of current proposals to address issues

22. The ASA has now issued guidance on how products and services with links to coronavirus should be marketed³- including new rules that ads should not exploit consumers' fears over the virus to mislead them into buying a product - but we are concerned that voluntary standards and guidance are not effective as a regulatory tool to protect consumers from fake and fraudulent ads. While standards and guidance may be effective in incentivising some businesses to improve advertising standards, it will not be effective in stopping scammers. Further action is required to prevent fake and fraudulent ads appearing in the first place.

Misinformation and the 5G network

The nature of the problem during the Covid-19 period

³ <https://www.asa.org.uk/news/coronavirus-covid-19-advertising-responsibly.html>

23. The deployment of 5G infrastructure had raised health concerns even before the pandemic, specifically concerns about the health risk from the potentially higher exposure to radiofrequency electromagnetic radiation arising from 5G networks.

24. Ofcom has been carrying out radiofrequency electromagnetic field measurements near mobile phone base stations, showing that electromagnetic field levels are well within the internationally agreed levels, and thereby disproving these theories. Public Health England has also said that as overall exposure to electromagnetic fields, including the 5G related ones, is expected to remain low “there should be no consequences for public health”⁴.

25. These fears have gained further prevalence as a result of fake theories connecting 5G and the spreading of Covid-19 in the UK and in the rest of the world. These have contributed to spreading fear and concerns over 5G, leading to masts being burned and engineers being harassed, both online and in person⁵.

Steps that have been taken to mitigate these concerns

26. Which? has emphasised that there is no correlation between coronavirus, 5G and health and supports the initiatives taken by Ofcom and the industry in fighting back against these claims⁶.

27. Ofcom has also launched its “Making Sense of Media Panel and Network”, which has collected a set of resources to help users to navigate and verify information on Covid-19. These resources include verified fact-checkers, such as Full Fact and Information, as well as information on how to seek out reliable content and spot disinformation⁷.

28. Steps have also been taken by the private sector, in particular social media platforms. Platforms like Facebook and Twitter have launched dedicated services to prioritise credible sources such as the NHS and the UK Government, while cooperating to limit the spread of hoax theories online. Other tech companies, such as Apple and Google have joined this endeavour to stop fake news over Covid-19 by prioritising stories from reputable sources.⁸ Furthermore, the four UK Mobile Network Operators issued a joint statement denouncing these theories as baseless, while also raising concerns that they are putting critical infrastructures, engineers and users at risk.⁹

⁴ Ofcom, Exposure to electromagnetic fields, 2020 <https://www.ofcom.org.uk/manage-your-licence/radiocommunication-licences/mobile-wireless-broadband/exposure-electro-magnetic-fields>

⁵ Ofcom, Clearing up the myths around 5G and the coronavirus, 2020, <https://www.ofcom.org.uk/about-ofcom/latest/features-and-news/clearing-up-myths-5g-and-coronavirus>

⁶ Which?, Is 5G safe? Everything you need to know on the 5G-powered future, 2020 <https://www.which.co.uk/news/2020/04/is-5g-safe-everything-you-need-to-know-on-the-5g-powered-future/>

⁷ Ofcom, Cutting through the Covid-19 confusion, 2020 <https://www.ofcom.org.uk/research-and-data/media-literacy-research/coronavirus-resources>

⁸ Ofcom, Cutting through the Covid-19 confusion, 2020 <https://www.ofcom.org.uk/research-and-data/media-literacy-research/coronavirus-resources>

⁹ EE, Vodafone, O2, Three, “Protecting Our Critical Infrastructure” 2020, https://uploads-ssl.webflow.com/5b7ab54b285deca6a63ee27b/5e8a14683d54a9d2f078baf8_MNO%20Statement.png

29. While this is a step in the right direction, it is clear that more needs to be done. According to a weekly series of surveys published by Ofcom, almost half of UK adults came across false or misleading information about coronavirus¹⁰. One of the most common pieces of misinformation respondents came across (from a select list) was 'theories linking the origins or causes of Covid-19 to 5G technology'.

The effectiveness of current Government proposals

30. Which? supports the Government's efforts to tackle the spread of hoax theories connecting 5G and Covid-19 such as the introduction of the **Government Coronavirus Information Service** on WhatsApp. However, to date initiatives to tackle the spread of misinformation related to 5G have been largely industry-led.

Price gouging and online platforms

The nature of the problem during the Covid-19 period

31. The coronavirus crisis has created very high demand for some consumer goods and this has created conditions in which profiteering and price gouging can thrive. The Competition and Markets Authority (CMA) and the Government have issued stark warnings against such practice, and the regulator has instigated an investigation into price gouging as part of its Coronavirus taskforce, threatening to take strong action if the problem persists.

32. Following reports of profiteering on products in high demand during the coronavirus pandemic, we have found persistent price gouging on essential items, and collated evidence through consumer research, investigations and launching a price gouging reporting tool. The price increases reported by consumers using Which?'s tool are significant, and specifically for hygiene and personal care products where there was a median price increase of 300%. Worryingly, almost a third (32%) of consumers who reported issues are buying products even when they believe the prices to be unfair.

33. In particular, our investigations have discovered widespread examples of price gouging on online marketplaces and the sale of essential items on auctions, and almost 60% of reports to Which?'s price gouging reporting tool relating to online marketplaces. Despite assurances from online marketplaces that effective measures are in place to block and remove the type of listings we identified, simple searches reveal how some traders are still managing to list basic goods for excessive prices, suggesting that the platforms' efforts are not effective enough.

Steps that could be taken to mitigate these concerns

34. It is clear that the existing regulatory tools to address this problem are ill-suited to the current situation. Depending on how goods are being sold, traders could be breaching the Consumer Protection from Unfair Trading Regulations 2008, which prohibit unfair and aggressive commercial practices as well as misleading actions. However, we are concerned that the legal framework available to enforcement agencies such as the CMA and Trading Standards is not suitable for tackling the problem of price gouging swiftly and effectively.

¹⁰ Ofcom, Covid-19 news and information: consumption and attitudes, 2020
https://www.ofcom.org.uk/research-and-data/tv-radio-and-on-demand/news-media/coronavirus-news-consumption-attitudes-behaviour#accordion_target-195349

35. We strongly believe that the UK is lagging behind its international counterparts and leaving consumers unprotected against exploitative profiteering during this crisis. It is our view that urgent legislation is needed to empower regulators to bring in timely and more effective interventions to restrict unjustifiable high prices of essential products during the current pandemic and future emergencies.

May 2020