# ABI response to Ofcom Illegal Harms consultation

***About Us***

*The ABI is the voice of the UK's world-leading insurance and long-term savings industry, which is the largest sector in Europe and the third largest in the world. We represent more than **300 firms within our membership**, including most household names and specialist providers, providing peace of mind to customers across the UK.*

*We are a purpose-led organisation: **Together, driving change to protect and build a thriving society**. On behalf of our members, we work closely with the UK's governments, HM Treasury, regulators, consumer organisations and NGOs, to help ensure that our industry is **trusted by customers**, is **invested in people and planet**, and can **drive growth and innovation through an effective market**.*

*A productive and inclusive sector, our industry supports towns and cities across Britain in building a balanced and innovative economy, employing over **300,000** individuals in high-skilled, lifelong careers, two-thirds of whom are outside of London. Our members manage investments of **£1.5 trillion**, pay over **£17.2 billion** in taxes to the Government and support communities and businesses across the UK.*

## Introduction

1. We are pleased that Ofcom recognises that online harms, such as fraud, have far-reaching consequences – carrying psychological as well as economic impacts. Both the insurance and long-term savings sectors are impacted by financial scams perpetrated via user generated content and paid-for advertisements. The problem has been exacerbated by, and ongoing since, the pandemic as people looked at ways of boosting their income or returns through attractive investment opportunities or making savings by securing cheaper motor insurance.
2. We strongly support government action aimed at improving online safety standards. Such action is essential for the UK to continue to develop, adapt and strengthen its response to online threats and meet the government's aspiration to become the safest place in the world to be online.
3. We broadly welcome the proposals outlined in the consultation and have no major concerns with them. As our primary interest is in initiatives designed to combat online scam adverts, we have focused our comments on the specific measures aimed at tackling and deterring fraud.

## Comments on fraud specific measures

### *Automatic keyword search*

4. We agree with the proposal that services that are at medium or high risk of fraud should put in place standard keyword detection technology to identify content that is likely to amount to a priority offence concerning articles for use in frauds (such as content which offers to supply individuals' stolen personal or financial credentials).
5. Data and identity theft are types of enabling activity that allow insurance fraud to be committed. Stolen credentials, often acquired over internet services, can be used to facilitate both application and claims insurance fraud, most prominently ghost broking.
6. Ghost broking is a common type of insurance fraud. The term is used to capture the range of tactics used by fraudsters to sell fraudulent motor insurance policies. Ghost broking is typically undertaken using social media, with fraudsters enticing victims by offering 'discounted' but fraudulent insurance policies. Ghost broking is typically carried out in one of three ways: fraudsters will either forge insurance documents; falsify details to reduce premium (using stolen personal or financial credentials); or take out a genuine policy before cancelling it soon after and claiming the premium refund plus the victim's

money.

7. We therefore support this proposal as this will enable services to identify content that could be used for fraudulent purposes. However, it is important that services take appropriate action when they detect content. We believe Ofcom could go further and make it a requirement that services remove content, not just leave it to the discretion of the individual service and its own content moderation policies.

8. Additionally, the consultation makes no reference to using technology to identify videos or images (such as GIFs and memes) that are commonly used on services by fraudsters to entice victims and avoid automatic keyword detection technology. We are aware that services have the ability to automatically fact check images, so they should be equally able to adopt the same technology to identify fraudulent content in the form of images.

### *Streamlined expert reporting*

9. We agree with establishing and maintaining a dedicated reporting channel for fraud for trusted flaggers. We believe a dedicated reporting channel will improve detection of illegal content and reduce harm to users by reducing difficulties organisations with expertise in fraud have in reporting known scams to services.

10. However, we would strongly assert that both the Insurance Fraud Enforcement Department (IFED) and the Insurance Fraud Bureau (IFB) should be specifically included/named as ‘trusted flaggers’. Both these organisations have expertise, knowledge and experience in detecting and investigating fraud.

11. IFED is a specialist police unit dedicated to tackling insurance fraud. Established in 2012, IFED is funded by the ABI and is hosted by the City of London Police (in much the same way as the Dedicated Card Payment Crime Unit [DCPCU] is funded by UK Finance). IFED's team of detectives, financial investigators and police staff act with operational independence while working closely with the insurance industry. IFED targets established criminality, including organised motor insurance fraud, while at the same time focusing on emerging threats. Since IFED’s inception in 2012, they have carried out over 2930 arrests, secured 584 convictions and 1418 other judicial outcomes amounting to over 310 years of prison time. Whilst IFED sits within the City of London Police, which is currently listed as a ‘trusted flagger’, given IFED’s status as a bespoke fraud unit, there is merit in allowing it to report directly (in much the same way as is proposed for the DCPCU).

12. The IFB is a not-for-profit company established in 2006 focused on the detection and prevention of organised fraud. The IFB supports the insurance industry and law enforcement by providing intelligence and assisting in investigations. The IFB also raises public awareness of insurance fraud scams: how they work and how to spot them, so that the chances of consumers being caught out are reduced. Since 2006, the IFB has assisted the police in making over 1300 arrests and securing 670 convictions that have resulted in around 600 years custodial sentences.

13. IFED and the IFB have taken proactive measures to mitigate the threat posed by online harms, through consumer awareness campaigns, intelligence sharing and cross-industry engagement. The IFB recently launched a joint campaign with Aviva aimed at helping raise awareness among consumers of paid-ad spoofing scams and how to avoid falling victim to them.[1] In 2021, IFED launched Operation Mirage, its first online disruptions initiative, in collaboration with the National Fraud Intelligence Bureau, the IFB and social media companies. This initiative aims to disrupt online fraudsters by taking down websites or social media profiles that are being used to carry out fraud. In 2023, IFED successfully disrupted 113 fraudsters by taking down social media accounts, websites, emails and issuing cease and desist notices to entities linked to insurance fraud.

### *Verified accounts*

14. We agree with the proposals that services should have, and consistently apply, clear internal policies for operating notable user verification / paid-for user verification schemes and improve public transparency for users about what verified status means in practice. As the consultation identifies, impersonation fraud online is a significant problem and causes a range of harms to individuals. Within the insurance and long-term savings industry, we have observed the following types of impersonation fraud:

    *Clone Investment scams*

15. These scams occur when an investor is duped into believing that they are purchasing a genuine investment product from a reputable brand (the website of which has been cloned and it is in fact a fraudster impersonating the reputable brand). Many insurers, banks and investment firms have been impacted, with scammers often using real employee names to reassure victims, many of which will be vulnerable inexperienced investors (rather than existing customers).

[1] https://www.youtube.com/watch?v=eBeAxpisI6k

*Google Ad Spoofing*

16. Following a road traffic accident, vulnerable motorists initiating a claim from the roadside on their smart phone are having their claims ‘hijacked’ by claims management services (CMS). Motorists are led to believe they are speaking to their insurer through evasive answers to questions or misleading websites. Scammers use psychological tactics to befriend, reassure and pressure victims at a time of stress, while all the time collecting personal information for financial gain.[2]

17. The impact of these scams is significant and wide-ranging. Victims can be induced to enter into funding agreements where the CMS will take a sizeable cut of any damages awarded (e.g. up to 35%); unfavourable credit hire agreements (with rates 90% higher); inflated car recovery and storage fees; payment of unnecessary excesses to the repairer; fabricated rehabilitation fees; some victims can have their vehicles sold for salvage without consent; and others have incurred speeding fines relating to a time that the vehicle was supposed to be under repair/in storage.

18. We note that prior to the Online Safety Act becoming law, some technology and social media organisations had begun to implement due diligence measures designed to tackle impersonation fraud, prevent online scam advertisements and offer protection against fraudsters using social media. For example, Google introduced measures that aim to ensure that advertisers are properly vetted before adverts are posted and that financial services firms verify their identity with the regulator (FCA) before advertising on the Google platform. However, the measures were ad hoc and tended to be specific to a particular organisation. Therefore, Ofcom’s proposal is a further step in the right direction as it will build on these measures by helping users identify potentially fraudulent content. Alongside this, clear guidance from Ofcom to services on what features an internal policy and associated processes should include for verification schemes will help ensure more consistency across services.

19. However, we note that the proposal only applies to those services who already operate user verification schemes. There is no requirement for services that don’t currently operate verification schemes to begin doing so. This potentially leaves those users of services without verification schemes vulnerable to fraud, as when controls are tightened in one area, fraudsters will look to exploit opportunities in another, where they perceive controls may not be as well developed. We would therefore suggest that Ofcom should also require services to establish and maintain a notable user verification system that meets certain criteria (where they do not already operate one).

20. Additionally, at present there are some services that only provide user verification for a fee. There would be greater consumer protection if verification was done free of charge and as matter of course, as part of a service’s duty to protect their customers from misuse of their service. If not, it would create loopholes in which fraudsters will operate.

21. The financial services sector has for many years faced difficulties with fraudsters utilising Companies House to set up fake companies that appear to have a degree of legitimacy about them. Identity verification of a commercial entity should be more than just a check that the corporation exists and is registered on Companies House. Ofcom should consider a commitment from services to review their anti-money laundering and sanction screening of corporate customers, if not already covered by current legislation or regulation. A superficial view of a corporation is insufficient to properly scrutinise the bona fides of a corporation or those involved in it and will allow criminal entities to operate in the virtual space.

## General comments on other measures

### *Content moderation, accountability and governance*

22. We broadly agree with the other proposals set out in the consultation paper for user-to-user and search services. In particular, we welcome the proposals related to content moderation and accountability & governance. The harsh reality of online scams is that as soon as one URL is taken down, a new URL with a similar address will often take its place. Alternatively, the scammer will set up a new website using the name of a different provider, advertising a slightly different opportunity. In short, the issue moves so quickly that simply listing domains will always be outpaced by new domains emerging. We have long argued that this problem will only be mitigated by holding the technology companies fully to account and introducing an obligation for them to take down harmful content. We welcome the proposals that content moderation systems and processes are designed to take down illegal content swiftly. We further support services having a Code of Conduct for all staff that sets standards and expectations around protecting users from risks of illegal harm and must ensure staff receive training and materials that enable them to moderate content effectively.

[2] It would be useful if Ofcom could provide clarity on whether this type of activity would constitute a fraud offence and be captured under the Online Safety Act. While offences in the Fraud Act 2006 and Financial Services and Markets Act 2000 are included as Priority Offences under the Online Safety Act and thus are considered “illegal harms”, it is not clear whether Google Ad Spoofing falls within these offences given scammers are not making a direct false representation and are often FCA registered firms.

23. However, as previously mentioned, we believe Ofcom could go further and make it an obligation that services remove content, not just leave it to the discretion of the individual service and its own content moderation policies. The current approach of services to complaints of false information, hate speech and other illegal harms is inconsistent and varies depending on the platform. This inconsistency creates a gap that fraudsters do and will continue to exploit, so a baseline by Ofcom that services must remove content is necessary.

### *Joined-up approach to regulation of the digital economy*

24. It is imperative that Ofcom is equipped with both adequate resources and technical expertise  to regulate the new regime effectively and has developed networks that enable it to engage and cooperate effectively with other regulators with online expertise so that there is a fully joined-up approach to the digital economy. The creation of the Digital Regulation Cooperation Forum - comprised of OFCOM, the Competition and Markets Authority and the Information Commissioner's Office - is a positive step forward for regulatory dialogue in the digital arena. The UK Plan for Digital Regulation, which sets out the government's overall vision for governing digital technologies should also help to shape a more coherent regulatory landscape.

### *Whole system approach to tackling online fraud*

25. The proposals outlined in the consultation will not stop fraudsters from using other approaches to commit fraud, such as using cold calling. It is therefore imperative that Ofcom's measures work in tandem with government action to prevent fraud (such as extension of the proposed ban on cold calling announced in the UK Fraud Strategy), commitments within the Online Fraud Charter, the proposed Online Advertising Programme and FCA action in relation to social media advertising.

26. While we acknowledge that it will take Ofcom some time to implement the regulatory regime in full, it is important that it meets its deadlines on the most important areas, notably illegal harms and protecting children. We therefore fully endorse the recommendations outlined in the Public Accounts Committee report: *Preparedness for online safety regulation* that Ofcom must meet its deadline to introduce codes of practice related to illegal harms within 18 months.[3]

27. It is imperative that users of services are aware of threats posed by illegal harms. The House of Lords Fraud Act 2006 and Digital Fraud Committee's report: *Fighting Fraud: Breaking the Chain* found that public awareness campaigns are a crucial part of the fight against fraud.[4] Ofcom should consider a coordinated publicity campaign or a commitment from all services to regularly publicise campaigns raising awareness of the threats of online fraud. They should also consider making available accessible 'awareness material', which has a particular focus on providing the most vulnerable in society with an understanding of online fraud, what illegal harms are and how they can protect themselves. There is presently very little material available and in many cases it has been left to charitable organisations to utilise their resources to educate consumers.

[3] https://publications.parliament.uk/pa/cm5804/cmselect/cmpubacc/73/report.html

[4] https://committees.parliament.uk/publications/31584/documents/177260/default/