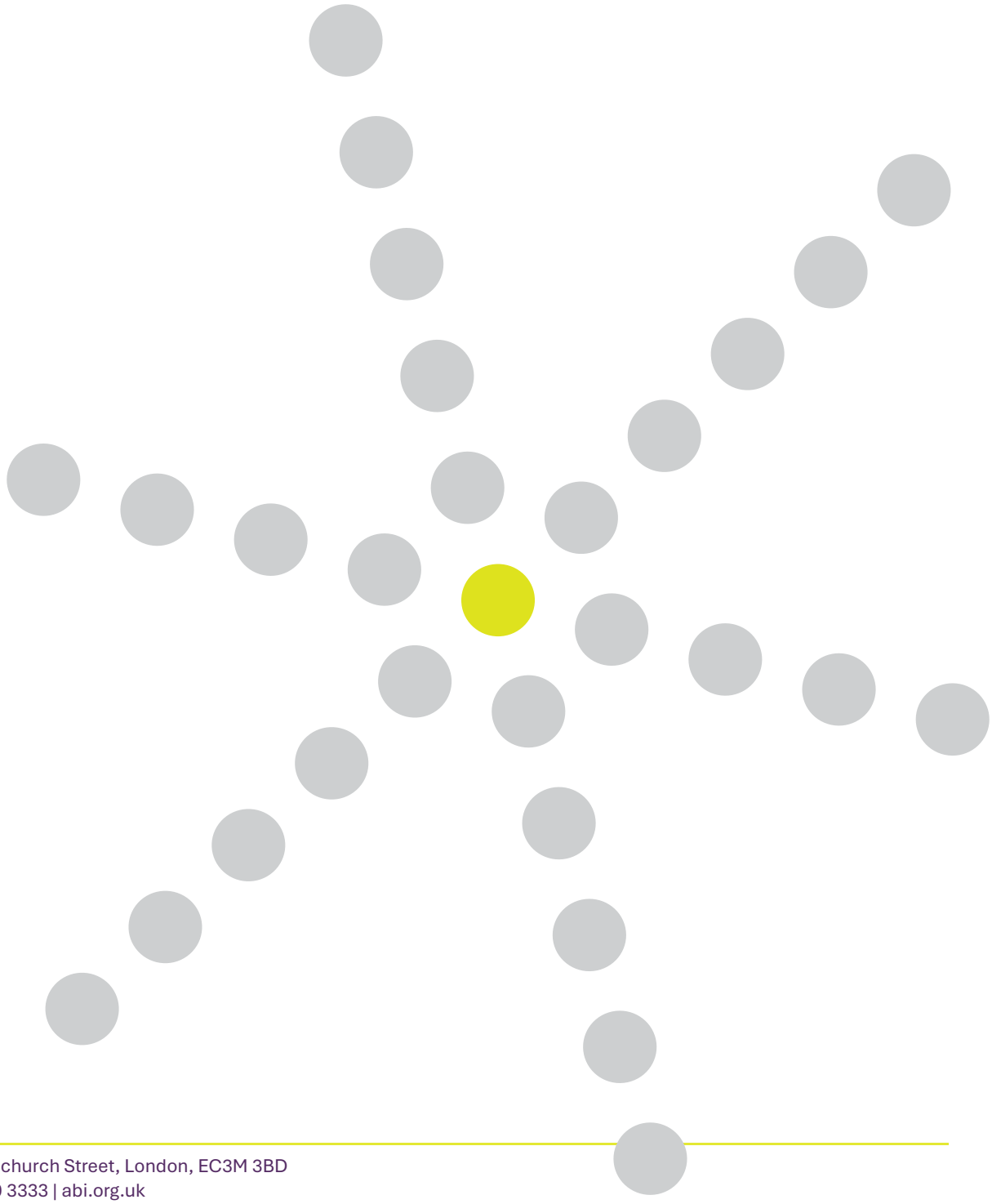
The ABI
Together Driving Change

The ABI response to Ofcom consultation on fraudulent advertising codes of practice

October 2026



The ABI | 30 Fenchurch Street, London, EC3M 3BD
T +44 (0)207 600 3333 | abi.org.uk

Introduction

1. Fraud remains a systemic threat costing the UK economy billions every year and causing major emotional and psychological harm to victims. It now constitutes over 46% of all crime across England and Wales, 67% of which is cyber enabled. Both the insurance and long-term savings sectors continue to be impacted by financial scams perpetrated online and fraudulent advertising is one of the central tactics used by criminals to target victims. Hence, we have an integral interest in ensuring strong action is taken to keep internet users safe and improves online safety standards.

2. While the Online Safety Act should deliver a major step up in protections for UK consumers against online fraud, its effectiveness will be undermined if the Fraudulent Advertising Codes of Practice lack teeth. Ofcom must use these Codes to hold technology companies and online platforms to account for the fraudulent content allowed on their platforms. We broadly welcome Ofcom's proposed Fraudulent Advertising Codes of Practice and support the overall direction of the framework. We particularly welcome the measures relating to mandatory verification of financial services advertisers, fraud indicator assessments, account integrity controls, trusted flagger mechanisms and testing of AI-enabled advertising tools. It is imperative that these measures are kept in the final version of the Codes in order for them to have any meaningful impact.

3. The Online Safety Act received Royal Assent in 2023, but Ofcom does not currently expect to publish its final Statement until mid-2027 at the latest. During this period, fraudulent advertisements will continue to expose consumers to financial, emotional and wider harm, so the Codes should be finalised and implemented as quickly as possible.

4. Tackling fraudulent advertising is essential to protecting consumers, maintaining public trust, and containing costs across the financial system. The most effective approach will be one that not only removes fraudulent advertisements once identified but prevents them reaching consumers in the first place. Together, the measures in the Codes represent a significant step towards achieving this approach, by making online platforms safer by design, reducing consumer harm and increasing platform accountability for fraudulent advertising. However, there are several areas where the proposed measures could be strengthened and outcomes-focused to improve their effectiveness and further reduce opportunities for criminals to exploit online advertising channels. Notably, the framework would be strengthened further through greater recognition of specific insurance fraud threats, stronger identity verification, more robust fraud indicator requirements, greater use of industry intelligence, stronger ongoing monitoring expectations, faster takedown standards and increased transparency.

5. It has become clear that insurers and banks continue to bear the majority of the financial burden for disrupting fraud. It is important that a collaborative, whole system approach is taken to tackling fraud. The technology and telecommunication must make a proportionate financial contribution to tackling fraud. We would echo the findings of the Independent Review of Disclosure and Fraud Offences that corporate accountability for online platforms must be strengthened through extending the 'failure to prevent fraud' offence to these sectors and imposing an anti-fraud levy on them to ensure that those whose systems are exploited contribute proportionally to enforcement and victim support.

Greater recognition of specific insurance fraud threats

6. We would encourage Ofcom to include insurance-specific examples in relevant guidance and illustrative materials accompanying the Codes. The following insurance fraud typologies represent the most prevalent kinds of fraudulent advertising activity on online platforms:

Ghost broking

7. Ghost broking is the most prominent type of fraudulent advertising activity affecting the insurance industry. Ghost broking is used to capture the range of tactics used by fraudsters to sell fraudulent insurance policies. It is typically undertaken on platforms such as Instagram, Facebook and TikTok, with fraudsters enticing victims by advertising 'discounted' but fraudulent motor insurance policies. Ghost broking is typically carried out in one of three ways: fraudsters will either forge insurance documents, falsify details to reduce premiums, or take out a genuine policy before cancelling it soon after and claiming the premium refund plus the victim's money. These are often accompanied by screenshots of the fraudulently obtained quotes and/or policy documentation.

8. The harms and consequences caused by ghost brokers can be far-reaching. As well as the financial loss associated with purchasing a fraudulent policy, many people who have fallen victim to a ghost broker won't realise their policy isn't genuine until they're stopped by the police or try to make a claim. Victims may face high costs in the event of an accident – paying out of pocket for their losses and then having to buy valid insurance. Those driving without valid insurance can also have their car seized and even crushed, face an unlimited fine and receive a driving ban.

9. Ghost broking is a significant and persistent form of fraud that aligns closely with several risk themes within the consultation including impersonation of trusted brands, misleading advertiser identities, suspicious account behaviour, fraudulent financial promotions and false claims of authority. This has already been recognised by other regulators and law enforcement agencies, notably the Financial Crime Authority who ran a campaign to raise awareness of ghost broking among young drivers and the Online Crime Centre who are running a ghost broking sprint. Therefore, we recommend that ghost broking is explicitly recognised as a fraud indicator and case study within the guidance. Verification should assess not only whether an insurer is legitimate, but whether the advertiser has genuine authority to sell, arrange, introduce or promote insurance products.

Paid Ad Spoofing

10. Another prominent type of scam advertising is Paid Ad Spoofing. Following a road traffic accident, vulnerable motorists initiating a claim from the roadside on their smartphone are having their claims 'hijacked' by rogue claims or accident management firms 'impersonating' their insurer through misleading telephone numbers or websites. Firms use paid advertising to appear at the top of search engine results when motorists search for their insurer to report a claim.[1] Scammers use psychological tactics to befriend, reassure and pressure victims at a time of stress, while collecting personal information for financial gain.

[1] Advertisements may falsely imply an association with an insurer, suggest a customer is automatically entitled to compensation, misrepresent regulatory status, disguise lead generation / data collection activity, misuse insurer branding/terminology or harvest personal information for subsequent misuse.

11. The impact of these scams is significant and wide-ranging. Victims can be induced to enter into funding agreements under which the firm takes a sizeable cut of any damages awarded; accept unfavourable credit hire agreements with significantly higher rates; pay inflated car recovery and storage fees, unnecessary excesses to the repairer, or fabricated rehabilitation fees; or allow their vehicles to be sold for salvage without consent. Others have incurred speeding fines relating to periods when their vehicles were supposed to be under repair or in storage.

Clone Investment Scams

12. Brand abuse is a prominent type of fraudulent advertising affecting the long-term savings industry. These scams occur when an investor is duped into believing that they are purchasing a genuine investment product from a reputable brand; the advert and any associated websites or documentation may appear to be from the brand. Many insurers have been affected, with scammers often using real employee names, including those of senior leaders, to reassure victims, many of whom will be vulnerable, inexperienced investors rather than existing customers. These scams can have a hugely detrimental impact on victims, with consumers potentially being defrauded of life-changing sums, the businesses impersonated suffering reputational damage, and trust in the financial services industry decreasing.

Strengthening advertiser and domain verification

13. We strongly support the proposed advertiser verification requirements and the specific requirement to verify that financial services advertisers are authorised before advertisements are published.

14. However, verification should go beyond confirming that a firm exists or appears on a regulatory register. Fraudsters frequently exploit legitimate company registrations, cloned firms, and other forms of false representation to create credibility. Platforms should therefore take reasonable steps to verify the identity of the advertiser, their authority to act on behalf of the organisation being advertised, the ownership and legitimacy of associated domains and websites and the relationship between the advertiser and any regulated entity referenced within the advertisement.

15. Consideration should also be given to stronger controls over domain registration. Currently, domains can often be registered with limited identity checks, creating opportunities for fraudsters to establish convincing online infrastructure quickly and anonymously. For financial services advertising, platforms should take reasonable steps to identify cloned firms and impersonation of authorised entities, rather than relying solely on verification that a genuine firm exists.

Enhancing fraud indicator assessments and preventative controls

16. We welcome Ofcom's proposal requiring platforms to undertake fraud indicator assessments and maintain indicators associated with high-risk advertisers and advertising activity.

17. The assessments could be further improved by placing greater emphasis on proactive, risk-based fraud prevention before advertisements are published. The consultation rightly identifies brand impersonation as a key example of an indicator of fraudulent advertising. Other indicators include cloned firms, ghost broking, misleading claims management advertising, unusually low-priced financial products, suspicious domains and URLs, rapidly changing advertiser information, movement of consumers to private messaging channels, false claims of authorisation or regulatory approval and

indicators identified through law enforcement and industry intelligence. Preventative controls informed by such indicators are likely to be considerably more effective than relying on post-publication reporting and removal.

Greater use of industry intelligence

18. We agree that providers should review relevant evidence from trusted flaggers and independent experts in fraudulent advertising. The proposed fraud indicator framework would also be strengthened by requiring platforms to utilise relevant fraud intelligence and emerging threat information from trusted external sources. There are several fraud resources which could be used by providers to enable them to understand their fraud exposure. These could include their own MI of identified frauds on their platform, national law enforcement data (such as from the NCA or Report Fraud) and industry data (such as from Cifas).

19. Fraud typologies change rapidly and are frequently identified first by financial institutions, law enforcement agencies and fraud prevention specialists. Consideration should therefore be given to mechanisms that support lawful intelligence sharing between online service providers, regulators, law enforcement agencies, financial institutions and other trusted industry participants. We particularly support development of arrangements that enable platforms to act on intelligence received from regulated firms which are often best placed to identify emerging abuse of their brands and customers, such as Meta's Fraud Intelligence Reciprocal Exchange with the banking sector.

20. Ofcom should encourage platforms to extend such existing intelligence sharing initiatives to other sectors, including insurance. The general insurance sector has invested heavily over many years in building a robust data-sharing infrastructure to help combat fraud, spearheaded by the industry's data sharing centre of excellence, the Insurance Fraud Bureau (IFB), which could provide value insight into the online fraud threat. This infrastructure includes databases containing records of suspected general insurance fraud (IFiHUB) and confirmed fraud cases (Insurance Fraud Register). Greater reciprocal data and intelligence sharing between online platforms and insurers would go some way to overcoming barriers to information sharing and building a whole system data driven response to tackling online fraud.

Ongoing monitoring and account integrity

21. Currently, it is far too easy for criminals to set up advertiser accounts and publish fraudulent adverts on online platforms. Therefore, we support Ofcom's proposed account integrity measures, including identity checks, account creation controls and identification of repeat offenders.

22. However, fraudsters are experts at discovering and exploiting loopholes in regulations, so advertiser verification should not be treated as a single onboarding event. Fraudsters frequently satisfy initial verification requirements before subsequently altering websites, removing ownership information, changing content, or adapting behaviour after approval has been granted. We therefore encourage Ofcom to strengthen expectations around ongoing monitoring and review throughout the lifecycle of an advertising account.

23. Platforms should be expected to periodically re-verify high-risk advertisers, continuously monitor changes to associated websites and domains, identify suspicious advertiser behaviour, reassess risk

where fraud indicators emerge and identify linked accounts associated with previously removed advertisers.

24. Criminals are not only adept at setting up their own accounts, but also at taking control of legitimate ones. Fraudsters who have been removed from accounts can often return with ease. Therefore, we support the measures outlined to counter account takeover. The Codes must oblige platforms to take measures to prevent scammers from returning or from simply switching to dormant accounts from which they can continue to target consumers.

AI-enabled advertising and fraud detection

25. We welcome the requirement for platforms offering AI advertisement-generation tools to assess and mitigate potential fraud risks associated with those tools. We would encourage Ofcom to go further by promoting the use of AI and machine learning not only to assess platform-generated tools, but also to proactively identify, quarantine and investigate potentially fraudulent advertisements before publication and throughout the lifespan of an advertising campaign. Modern detection technologies can identify patterns associated with brand impersonation, misleading content and emerging fraud typologies at a scale not achievable through manual review alone.

Accountability across the advertising ecosystem

26. We believe that where Category 1 and Category 2A providers utilise advertising intermediaries, marketplaces, affiliates or other third parties, responsibility for consumer outcomes should remain with the platform provider. Consumers are unlikely to understand the complexity and opacity of online advertising supply chains. Accordingly, platforms should maintain sufficient oversight and control to ensure that fraud prevention measures are consistently applied throughout the advertising ecosystem. Greater transparency regarding advertiser ownership and responsibility would also support effective enforcement where harm occurs.

Faster response to trusted flagger reports

27. We agree with proposals relating to reporting mechanisms and establishing a dedicated reporting channel related to fraudulent advertising for trusted flaggers. A dedicated reporting channel will improve detection of fraudulent advertising and reduce harm to users by reducing difficulties organisations with expertise in fraud have in reporting known adverts to services.

28. The framework would benefit significantly from defined service expectations for handling verified fraud reports. Where regulated firms, law enforcement agencies or recognised trusted flaggers identify fraudulent advertisements, platforms should be expected to investigate and remove such content within clearly defined timescales. Fraudulent advertisements can generate significant consumer harm within a short period and therefore rapid disruption is critical.

29. We also strongly assert that both the Insurance Fraud Enforcement Department and the Insurance Fraud Bureau should be specifically named within the Codes as trusted flaggers. Both these organisations have expertise, knowledge and experience in detecting and investigating fraud.

30. IFED is a specialist police unit dedicated to tackling insurance fraud. Established in 2012, IFED is funded by the ABI and 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, they have carried out over 3559 arrests and voluntary attendance interviews, secured 708 convictions and prison sentences worth a total of 408 years. Whilst IFED sits with 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). It should be directly referenced in FAU D7.2 - *the City of London police force (which includes the Dedicated Card and Payment Crime Unit (a joint team of the City of London and Metropolitan police forces) and the Insurance Fraud Enforcement Department).*

31. The IFB is a not-for-profit company established in 2006 focused on the detection and prevention of organised fraud. The IFB is a Specified Anti-Fraud Organisation that 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 has resulted in around 600 years of custodial sentences.

32. IFED and the IFB have taken proactive measures to mitigate the threat posed by fraudulent advertising through consumer awareness campaigns, intelligence sharing and cross-industry engagement. 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 ongoing initiative aims to disrupt online fraudsters by taking down websites or social media profiles that are being used to carry out fraud. In 2025, IFED successfully disrupted 136 fraudsters by taking down social media accounts, websites, emails and issuing cease and desist notices to entities linked to insurance fraud.

33. Ofcom should consider developing a mechanism through which other organisations can become trusted flaggers. Due to the rapidity of turnover of paid adverts, speed of response can be key in flagging concerns, and we would therefore suggest that insurers are also provided a pathway to becoming trusted flaggers if possible. Insurers proactively identify these adverts on a daily basis and utilising a conduit for flagging to online platforms could cause delays which could negate a significant amount of the potential benefit of the proposals.

Consumer transparency and reporting

34. We support Ofcom's proposals for user reporting systems and advertising transparency measures, including advertising libraries.

35. Consumers would benefit from greater visibility regarding advertiser verification and fraud prevention controls. For example, platforms could provide verification indicators or trust markers showing the level of validation undertaken. Ofcom should also consider creating a public record of detected and removed fraudulent adverts. Consumers, researchers and regulators should be able to identify fraudulent adverts, study tactics used by scammers and ensure that platforms are complying with their duties to remove scam adverts.

36. Many consumers do not report scams because they do not know how. Failure to report scams not only increases the possibility of further consumer harm, but also means platforms have less information

from which to draw when refining the content moderation systems. Consumer reporting processes should be straightforward, accessible, and proportionate. We encourage platforms to provide users with appropriate feedback on the outcome of reports wherever possible, which may improve trust and encourage further reporting.

Measuring effectiveness

37. To assist assessment of effectiveness, consideration should be given to requiring platforms to publish performance measures relating to fraudulent advertising, including detection rates, advertiser verification rates, removal times, response times to trusted flagger referrals, repeat offender rates, appeals outcomes and account suspension and enforcement activity. Publication of such information would improve transparency, support accountability, and allow regulators and stakeholders to assess whether the measures are delivering meaningful reductions in consumer harm.

Better regulatory coordination

38. It is imperative that Ofcom 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 and coordinated approach to online regulation. We encourage Ofcom to coordinate closely with the Financial Conduct Authority, Advertising Standards Agency, Home Office, law enforcement and industry bodies. Online scam advertising cuts across several regimes and fragmented regulation risks gaps, duplication or slow response.

About us

The ABI is the definitive 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.

Our sector is productive, inclusive and essential to the UK economy and together, we are driving change to protect and build a thriving society.

Find out more at **abi.org.uk**