Digital advertising industry commitment to tackle scam advertising online

This declaration made by the Internet Advertising Bureau (IAB UK) outlines our members' ongoing commitment to address the issue of financial scam advertising. We believe existing efforts can be strengthened through coordinated action by industry, regulators and law enforcement. This declaration follows a period of consultation which has drawn in feedback from IAB UK members across the digital advertising ecosystem drawing on their long-standing experience and expertise in responding to the threats posed by scam advertisers.

IAB UK and its members are actively engaged in informing the Home Office Fraud Action Plan and the DCMS Online Advertising Programme. It is our strong belief that these provide the best route to build on existing efforts and enable our members and their partners to dynamically respond to threats. Premature steps to legislate on this issue in haste may undermine live Government workstreams designed to fully assess the underlying issues and gather evidence to understand where existing efforts are effective and should be expanded, and where further, targeted solutions may be appropriate.

We propose a three-pronged approach based on:

a) strengthening coordinated industry efforts focused on prevention and disruption of criminal activity
b) raising consumer awareness of scams and providing strategies to respond, and
c) building on Government and regulator efforts to work with industry by developing intelligence-sharing mechanism to support law enforcement against criminal actors, for example through working with the National Economic Crime Centre.

We believe that, together, these represent the most effective next steps for combating the threat of scam advertising.

Below we outline why legislation is not the right solution to this kind of threat; what solutions our industry is committed to pursuing; and what role regulators should play in addressing this threat.

Recognising the nature of the problem

These scams are **financial crimes** committed primarily against individuals and against the advertising industry itself. The complexity of this ever-moving, ever-mutating challenge cannot be understated and it is essential that any expansion of existing efforts or new measures to tackle it draw on industry expertise rooted in an in-depth, practical knowledge of their impact on the online advertising ecosystem. That includes understanding the different digital advertising buying and delivery models (such as social media, search, open display, etc), how each may be exploited and the respective solutions that may be appropriate in each case. Evidence is also needed to understand the nature and volume of fraud occurring through different types of digital advertising models, in order to identify the most appropriate and effective solutions.

As the nature of scam ads evolves and the vectors of attack change, statutory legislation is insufficiently agile to combat future iterations. To this end, the industry believes that **creating a hostile environment** for sophisticated scammers and ensuring preparedness for future threats will be the most effective strategy for mitigating this issue.

Our industry's commitment to create a hostile environment for scammers

At the heart of scam advertising are highly organised, technically-sophisticated scammers who exploit online advertising to entrap people using a range of techniques which evolve quickly. Efforts to combat scam advertising fall within two core pillars of **restricting opportunity** and **disrupting bad actors**. IAB UK and the global industry standards body TAG[1] work with members to develop and disseminate good practice for the various business models in the digital ad ecosystem. This can include, for example:

> *Restricting opportunity*
> Having effective measures in place, such as appropriate tools and vetting procedures at the account set-up phase, to secure access to systems, spot suspicious actors/activity, and stop bad actors entering the advertising ecosystem.
>
> *Disrupting bad actors*
> Having effective methods in place to monitor active campaigns in order to detect behaviour indicative of criminal operation (such as IP cloaking), to share information with industry partners to allow firms to take pre-emptive action to disrupt criminals who may move between services.

In addition to individual company action, IAB Tech Lab[2] is actively developing new industry technical standards for buy-side transparency which, if adopted, will improve the likelihood of tracing the source of 'bad' ad creatives across platforms and of taking action to stop them.

The recently established Online Fraud Steering Group, supporting the Home Office's upcoming Fraud Action Plan, is also working to make the UK the least attractive place for online fraudsters to operate by increasing dialogue and collaboration between the banking and technology industries (including some digital advertising platforms) and law enforcement. The OFSG has expedited practical action with participants on system changes including in relation to the authorisation of advertisers.

Informing and empowering consumers

Raising consumer awareness of fraudulent advertising and providing methods for scams to be reported is also crucial. The Advertising Standards Authority (ASA) – which regulates good actors in the industry – has developed a 'Scam Ad Alert' initiative, in partnership with the major digital advertising intermediaries, publishers, and social media platforms to supplement individual company efforts. It gives consumers a means of reporting suspected scams that have appeared in paid-for spaces online to the ASA, and the ASA sharing alerts so firms can take appropriate action.

Additionally, the 'Take Five to Stop Fraud' campaign led by UK Finance represents an important initiative to increase consumer awareness about the types of fraudulent activity online, which many of the largest social media companies have pledged to support.

Our ask of government, regulators and law enforcement

The issue of advertising as a vector for scams is ripe for a coordinated response and this should include effective joint work between industry and functions of the state. For example, some industry members and IAB UK are in discussion with the FCA about how best its warning list can be used, including how it could be made available in a format that could be easily, quickly and automatically ingested into companies' systems. We also note that there are existing models for industry information-sharing with law enforcement in the US that could provide a useful basis for exploring closer partnership working in the UK. It is absolutely critical that law enforcement activity is appropriately prioritised and resourced to

[1] TAG Certified Against Malware sets standards for addressing "malvertising", which can include scam ads https://www.tagtoday.net/pressreleases/malware-certification

[2] Tech Lab is the global technical standards body for digital advertising https://iabtechlab.com/about-the-iab-tech-lab/

ensure that criminal actors face legal consequences for their actions.

This joint working needs to be based on a full and shared understanding of the nature and scale of the problem and how it manifests in different parts of the digital advertising ecosystem. Existing government workstreams need to devote sufficient time and attention to understanding and examining both the substance and quality of the industry response and what it has achieved, as well as the evolving criminal behaviour the industry experiences, to enable the development of evidence-led solutions.

It is also important that policy-makers and regulators give due consideration to the competition impacts and the potential unintended consequences of the different potential responses to scam ads, and to the impact of exercising legacy powers in digital markets.

Conclusion

Scam advertising is a devastating crime against consumers and legitimate advertising businesses alike. IAB UK is troubled by generalised assertions that the industry response as a whole has come late and falls short. The advertising industry has responded with both determination and creativity and we do not dispute that these efforts should evolve and be responsive to the changing patterns of criminal activity.

Together with government, regulators and law enforcement bodies, the UK digital advertising industry wants to play its part in restricting, detecting and disrupting scam ads. To be most impactful, work now should focus on gathering evidence to understand where existing efforts are effective and should be expanded, and where further, targeted solutions may be appropriate; improving intelligence-sharing; supporting consumers and pursuing criminal actors.

We would welcome the opportunity to engage with Ministers on the points raised in this industry declaration.