SUBMISSION TO OFCOM - FRAUDULENT ADVERTISING CONSULTATION ON BEHALF OF GUARDIAN NEWS AND MEDIA LTD (GNM)

Date:	2nd October 2026
Stakeholder:	Guardian News & Media Limited
Responding to:	Ofcom - Fraudulent Ads Consultation

—----------

Executive summary

Guardian News & Media Limited (GNM) supports Ofcom's decision to implement robust Codes of Practice tackling fraudulent advertising under the Online Safety Act. Premium news publishers depend directly on reader trust and high advertising standards. Fraudulent advertisements erode consumer confidence, inflict financial and emotional harm on readers, and unfairly damage the reputation of trusted news brands whose operational environment fraudsters actively exploit.

We support a strong, layered approach that closes the gap between direct advertising controls and third-party programmatic routes. The involvement of DSPs, SSPs, exchanges or agencies should not dilute responsibility or create a weaker safety outcome for users.

While GNM endorses Ofcom's emphasis on safety-by-design and account-level prevention, our operational experience reveals a number of areas that should be strengthened before final enactment.

- Define 'reasonable endeavours' to include contractual accountability along the ad supply chain
- Enforce strict legal deadlines for takedowns of high-harm scams
- Set minimum standards for complaints processes that include accessibility and human response to avoid automated rejections
- Focus on preventative measures such as verifying advertisers upfront to avoid the burden falling on publishers and readers
- Build safety into AI ad tools and review risks more often

Publishers can and should apply strong controls, but we are often not the party with the full advertiser relationship, account-level visibility or enforcement power. For third-party programmatic advertising, the only workable model is shared responsibility with clear

accountability at each point in the chain. Otherwise, publishers and users are left dealing with the harm after the ad has already appeared.

Question 1: The Online Advertising Ecosystem

The Guardian's advertising department supports the commercial funding of Guardian journalism across a broad mix of digital advertising routes, including direct-sold campaigns, programmatic guaranteed, PMP, open market programmatic, video, app, newsletters and partnership-led activity. The team works closely across Sales, Ad Operations, Digital Optimisation, Product, Data, Legal, Data Protection and Ad Quality to balance commercial delivery with reader trust, brand suitability, privacy and user experience.

A large proportion of digital advertising now runs through automated and programmatic channels, which means adverts can reach Guardian inventory through a number of different demand partners, platforms and intermediaries. We therefore operate a **layered approach to ad quality**, using contractual controls, blocklists, category exclusions, partner governance, ad verification, internal escalation routes and specialist ad quality technology to identify and remove problematic ads as quickly as possible.

Maintaining a safe and high-quality advertising environment is important not only for readers, but also for advertisers who choose us because of the strength and trust of our brand. **Fraudulent ads damage confidence in open-market advertising,** putting pressure on legitimate advertising relationships. It also creates **additional operational burden** for teams and diverts financial resources. In the Guardian's case, we have invested in real-time ad security technology to detect post-click cloaking and auto-redirects.

Our aim is to protect readers, protect the Guardian brand, and ensure that advertising remains a sustainable and responsible part of our commercial model, and to that end we welcome Ofcom's proactive engagement in this area.

Questions 2 & 3: Causes, Impacts, and Risky Characteristics

GNM endorses Ofcom's assessment of the severe financial and emotional harm caused by scam ads. Fraudsters deliberately target premium news environments to borrow credibility from trusted media brands, public figures, and topical news events (e.g., cost-of-living concerns, health trends, energy offers, and financial markets). Readers come to the Guardian expecting a trusted, high-quality environment, and **when a fraudulent or misleading advert appears on our site, even if it has entered through a third-party programmatic route, they may associate that experience with us.**

We also see how **scam tactics change quickly** in response to news cycles, seasonal trends and public attention. For example, fraudsters may use major financial stories, cost-of-living concerns, health trends, well-known consumer brands, energy-saving products or public figures to make the ad feel topical and legitimate. The common theme is that these ads are designed to look credible enough to gain a reader's trust before moving them into a potentially harmful environment.

Speed is another challenge. Scam ads can be short-lived and often move quickly across routes. By the time a complaint is received and investigated, the ad may have stopped serving, changed creative, or reappeared through a different buyer or platform. This is why **we need both preventative controls and fast escalation routes with partners,** rather than relying only on reader complaints after the ad has already appeared.

Questions 4 & 5: Approach to Codes, Timeframes, and Proportionate Burden

GNM strongly **supports Ofcom's emphasis on safety-by-design and proactive account integrity.** Given the societal impact of scam ads (estimated by the Home Office at £9.2bn per year), the proposed regulatory burden is largely proportionate. The deadline for the final statement is 9 months from when the consultation closes - we hope Ofcom will make every effort to pull this forward to the earliest possible time given that harms are current and ongoing.

Question 6: 'Insufficient Control' Exemption (FAU K1 / FAS K1)

Reasonable endeavours in third-party scenarios

Scenario 1 (DSPs and media agencies): Where the end-advertiser does not have a direct account with the platform, it may not be realistic for the publisher or platform to complete every onboarding check itself. However, that cannot become a loophole. We support the ambition that **compliance expectations should be passed upstream** through contracts, technical standards and active partner governance.

In practice that means that DSPs, agencies and demand partners should be required to apply equivalent advertiser verification, brand representation checks, financial services checks where relevant, and banned-account controls. **Platforms and publishers should also be able to refuse, suspend or restrict demand routes where buyer identity is unclear**, transparency is weak, or repeat issues are not addressed.

It should be stressed that **buyer identity needs to be actionable, not theoretical**. It is not enough to know that an ad came through a DSP or agency seat; publishers need

sufficient transparency to identify the buyer, advertiser, domain, creative and supply path involved so that issues can be escalated and suppressed quickly.

For scenario 2 (SSPs and open-display auctions) we recognise that **pre-screening every creative and landing page before it renders is not always practical** given the speed and complexity of real-time programmatic trading. However, **it is reasonable to expect a layered control framework**: strict category controls, blocklists, domain suppression, partner-level enforcement, and specialist ad security technology that can inspect creative behaviour, redirects and landing-page risk in real time.

One issue missing from the scenarios is how to deal with **harmful post-click behaviour.** Scam ads may look compliant at the point of bid or creative review, but the risk often appears through redirects, cloaked pages, device-specific behaviour or landing pages that change after approval. This makes detection more difficult because the version seen by a verification system or ad quality reviewer may not reflect a reader's experience. Reasonable endeavours therefore need to cover both the ad creative and the user journey after the click.

Potential loophole

Open-display programmatic ad networks represent one of the primary vectors through which fraudulent advertisements are distributed across the internet. If platforms can bypass strict compliance by claiming lack of direct control over intermediaries, bad actors will simply concentrate their scam campaigns within programmatic open-display channels.

To ensure this measure operates effectively and does not become a fallback for compliance failure, GNM suggests strengthening the code with specific operational standards.

Recommendations

- **Contractual cascade:** Ofcom must define "reasonable endeavours" to mean that platforms are legally required to contractually cascade compliance down through connected DSPs/SSPs. There is precedent in how the UK deals with bribery, money laundering or people trafficking for companies with a turnover over a certain threshold. It could include auditability, escalation rights, suspension rights and consequences for repeat failures. Contracts should also require partners to provide timely investigation data when issues occur, including buyer ID, advertiser name, domain, creative ID, deal ID, seat ID and any relevant reseller path.
- **Immediate supply-chain blocking:** When a fraudulent ad or bad buyer account is identified on an intermediary network, platforms should enforce global domain

and buyer ID suppression across all programmatic inventory. The caveat is that this needs to be precise enough to avoid over-blocking legitimate activity where an issue is isolated, spoofed or misattributed.

- **Repeat-offender intelligence sharing**. Bad actors often rotate between domains, accounts, DSP seats and supply paths. If one publisher or platform identifies a fraudulent pattern, there should be a faster way for that intelligence to flow through the ecosystem, rather than every publisher having to discover the same scam independently.

Question 7: Fraud Indicator Assessments & AI Tools

The current climate makes this particularly urgent because generative AI is making scam creative cheaper, faster and more convincing. Fake news-style creative, synthetic public figure endorsements, cloned brand assets and misleading "article" landing pages are becoming easier to produce at scale. Any reasonable framework needs to account for the fact that scam ads are no longer manually created one by one; they can be generated, varied and rotated quickly.

Recommendations:

- **Bi-annual Fraud Indicator Assessments** rather than annually given the speed of generative AI and deepfake development.
- Platforms offering AI ad-generation tools (FAU F1 / FAS F1) should be held liable if their proprietary AI tools' outputs do not have **guardrails to prevent brand-impersonating.** While this will not catch all AI tools, given that third-party tools that an advertiser independently chooses are excluded – we support testing of tools hosted by the service even if they are built and operated by a third-party supplier.

Questions 8–10: Verification, Account Takeovers & Advertising Bans

Stopping scam ads is difficult because the activity is deliberately evasive. Bad actors constantly change advertiser names, domains, creative, landing pages, supply routes and accounts to avoid detection. A blocked domain may reappear under a slightly different URL.

A banned advertiser may return through a new account. A scam landing page may only appear after a redirect or under certain conditions. This means the issue cannot be solved through one control alone.

GNM endorses Ofcom's focus on account-level prevention (FAU H1–H5). Stopping bad actors before they can create ad buyer accounts is the single most effective intervention in the supply chain.

- **Upfront advertiser verification** should be a baseline expectation, especially where ads use a brand, public figure, financial product or make a sensitive claim. This could be strengthened to include proof of authority where an advertiser is using a third-party brand, public figure or news-style creative.
- **Banned account controls** are important to stop bad actors simply reappearing under new names, though they need appropriate safeguards to avoid false positives and privacy issues. This should include linked account detection, payment method checks, domain ownership signals and rapid re-blocking where repeat behaviour is identified.
- **Financial services pre-verification**: Mandatory verification of FCA authorisation before any financial service or investment advertisement is permitted to serve to UK users.
- **Countering account takeover,** including MFA and rapid escalation for compromised accounts, should be treated as basic good practice. Platforms should have a clear emergency route for legitimate brands or publishers to report suspected account compromise, because hijacked accounts can carry a false sense of legitimacy.

Questions 11-12 Advertising Moderation & Takedown Windows

Proposed measures FAU C4/FAS C4 allow platforms to set their own internal performance targets for moderation. Ofcom should institute statutory tiered response times scaled by harm severity.

Recommendation: Impersonation of news organisations, journalists, or public institutions must carry a mandatory takedown SLA (e.g., within 2 hours of receipt of notification from a verified Trusted Flagger or verified brand owner) backed by statutory financial penalties for non-compliance.

Questions 13-14 Advertising Complaints & Trusted Flagger Channels

While complaint routes exist across most major platforms and ad partners, their **effectiveness varies widely**. Direct escalations with named contacts (via SSPs, DSPs, or ad quality vendors) are far more reliable than generic public forms, delivering faster action and clearer feedback.

The best complaint systems are the ones that are **easy to access, allow evidence to be submitted clearly, provide a fast route to a real operational team, and give meaningful feedback on the outcome.** It is not enough to submit a complaint into a generic form and receive no clear response. We need to know whether the ad was removed, the buyer or account blocked, the domain suppressed, and whether similar activity can reappear through the same route.

However, even good systems can be slower than the pace at which scam advertisers operate, which is why complaint handling needs to sit alongside preventative detection, real-time monitoring and stronger partner accountability. The burden of finding scams should not rest on readers or publishers.

Opposition to FAU D6 / FAS D6

Granting platforms the power to self-define dismissible complaints creates a potential conflict of interest, incentivising broad auto-filtering to reduce moderation overhead.

This model fails when confronted with sophisticated fraud tactics like post-click cloaking when bad actors serve benign creative, which masks the hidden redirects that scammers use to send mobile users to fake news websites. Because automated filters only see the harmless front layer, they are likely to dismiss legitimate publisher complaints as "unsubstantiated."

Recommendation: To protect trusted media brands and readers alike, Ofcom should explicitly mandate human operational review for all publisher- and brand-impersonation complaints. In a recent tangential case involving a deepfake of a Scottish politician[1], Meta's systems did not prioritise the post for human review even after the victim complained, prompting Meta's own oversight board to call for tougher financial penalties.

Public Ad Libraries & Hyper-Personalisation (FAU E1 / FAS E1)

GNM supports public ad libraries but highlights a major technical challenge regarding hyper-personalisation. Modern ad networks allow extreme micro-targeting based on niche

---

1 https://www.oversightboard.com/news/meta-must-do-more-against-harmful-deepfakes-containing-hate-speech/

demographics, specific postcodes, or tailored behavioural segments. Standard ad library keyword searches may fail to reveal localised or micro-targeted scam ads. Therefore we would back ad libraries providing an API to enable programmatic polling alongside standard web search functionalities.