Consultation response

Field	Value
Responder	Conscious Advertising Network (with University of Portsmouth)
Responder Type	organisation
Org Role	Head of Advocacy
Org Type	Civil society

Volume 1: Context

3. Online advertising ecosystem

Q1: Is there any information or evidence you hold that could enhance our understanding of the online advertising ecosystem?

The Conscious Advertising Network welcomes the opportunity to respond to this consultation. We have worked with Dr [redacted] from the University of Portsmouth to develop this response.

The Conscious Advertising Network (CAN) welcomes Ofcom's recognition of the scale and complexity of the online advertising ecosystem. We would, however, encourage Ofcom to give greater weight to opacity within the digital advertising supply chain as a systemic enabler of fraud, rather than considering fraudulent advertising primarily as a problem of individual fraudulent advertisements or advertising account (Science, Innovation and Technology Committee, 2025).

Programmatic advertising involves multiple intermediaries and highly automated transactions, often leaving advertisers with limited visibility over where advertisements appear, which entities receive advertising revenue, and how money moves through the supply chain. The House of Commons Science, Innovation and Technology Committee's 2025 report on Social media, misinformation and harmful algorithms described evidence that the digital advertising supply chain is 'excessively complex' (p.48). It cited the Incorporated Society of British Advertisers' (ISBA) evidence that an average programmatic campaign can involve approximately 9,000 websites, with brands consequently having limited ability to track where their advertisements and money ultimately go.

This opacity creates conditions in which fraud can flourish. It can prevent advertisers, researchers, civil society and regulators from identifying fraudulent actors and transactions, while making it harder for legitimate advertisers to determine whether their expenditure is reaching genuine audiences and legitimate publishers (Richet, 2022). Fraud should therefore be understood not simply as malicious content entering an otherwise transparent advertising system, but as a risk facilitated by structural characteristics of that system.

The precise scale of advertising fraud is inherently difficult to quantify, and estimates vary according to definitions and methodology. Nevertheless, available research indicates that the sums involved could be substantial. Juniper Research (2023), drawing on data covering digital advertising activity across 45 countries, estimated that 22% of global digital advertising spend - approximately US$84.2 billion - was lost to advertising fraud in 2023, and projected losses of US$172.3 billion by 2028. To illustrate the potential scale of such losses in a UK context, Interactive Advertising Bureau UK and PwC reported UK digital advertising expenditure of GBP16.5 billion in 2020 (IAB UK, 2021). If a loss equivalent to Juniper Research's global estimate of 22% were applied to that level of UK expenditure, this would equate to approximately GBP3.6 billion. This is an illustrative extrapolation rather than an estimate of actual UK advertising fraud losses, since

the prevalence of fraud varies by market, advertising channel and methodology.

The difficulty of producing reliable estimates itself highlights an important underlying problem. The opacity and complexity of the digital advertising ecosystem make it difficult for advertisers, regulators and researchers to establish how much advertising expenditure is being diverted through fraudulent activity, to whom that money ultimately flows, and at what points within the supply chain fraud occurs. Greater end-to-end transparency and access to auditable advertising data are therefore important not only for preventing and detecting fraud, but also for establishing its true economic scale. This approach is consistent with the UN Global Principles for Information Integrity (United Nations, 2024), which recommend end-to-end validation of the advertising technology supply chain, disclosure of full advertising campaign data including placement and blocking data at log level, thorough campaign audits, and independent third-party auditing and vetting of advertising exchange supply partners.
CAN therefore encourages Ofcom to place transparency and auditability at the centre of the Codes. In particular, providers should be expected, where proportionate and consistent with data protection requirements, to retain and make available sufficiently granular information to enable regulators and appropriately authorised independent researchers to establish:
* who purchased an advertisement and, where relevant, the beneficial owner or organisation ultimately responsible;
* which intermediaries participated in the transaction;
* where and when the advertisement was served;
* the targeting and distribution parameters applied;
* material changes made to advertising accounts, payment methods, domains or destination URLs;
* and, where relevant to investigating fraud, the flow of advertising payments and revenue.

Ad libraries are an important component of transparency infrastructure, but they should not be treated as a substitute for access to sufficiently granular underlying data. Research examining existing platform ad repositories has identified significant limitations in their functionality and usefulness for independent scrutiny (Mozilla Foundation, 2024). Public-facing libraries, regulator access and appropriately safeguarded researcher access perform different functions and should therefore be designed accordingly. The UN Global Principles for Information Integrity call for granular data on advertising placement and for ad-tech companies to provide clients and researchers with full campaign data, including placement and blocking data at log level (United Nations, 2024).

Ofcom should also recognise the relationship between fraudulent advertising and the wider problem of advertising fraud, including invalid traffic, fraudulent domains, 'made-for-advertising' (MFA) sites and other mechanisms through which advertising expenditure can be diverted to illegitimate actors. The harm extends beyond financial losses to advertisers: advertising revenue can create economic incentives for the production and dissemination of deceptive or harmful online content (Ahmad et al., 2024; Diaz Ruiz, 2024), while substantial advertising expenditure can also flow to low-quality made-for-advertising environments; ANA research found that 15% of programmatic advertising spend in its study went to MFA sites (Association of National Advertisers [ANA], 2023). These phenomena do not always fall within the statutory definition of a fraudulent advertisement under the Online Safety Act, but they form part of the same advertising infrastructure and can involve overlapping actors, techniques and financial incentives. Understanding these connections will be important to effective enforcement and to identifying displacement of fraudulent activity.

Finally, the regulatory landscape itself remains fragmented. Ofcom's responsibilities intersect with those of the FCA, ASA, CMA, ICO, law-enforcement agencies and other bodies concerned with fraud and economic crime. CAN recommends formal mechanisms for information-sharing and cross-regulatory coordination so that intelligence identified through implementation of these Codes can be acted upon across the wider fraud and advertising ecosystem.

References
Ahmad, W., Sen, A., Eesley, C., & Brynjolfsson, E. (2024). Companies inadvertently fund online misinformation despite consumer backlash. Nature, 630,

123-131.https://www.nature.com/articles/s41586-024-07404-1Association of National Advertisers. (2023, September 26). ANA programmatic media supply chain transparency study finds 15% of ad spend goes to made-for-advertising websites.https://www.ana.net/content/show/id/pr-2023-09-made-for-advertisingDiaz Ruiz, C. A. (2024). Disinformation and fake news as externalities of digital advertising: A close reading of sociotechnical imaginaries in programmatic advertising. Journal of Marketing Management, 40, 807-829.https://www.tandfonline.com/doi/full/10.1080/0267257X.2024.2421860IAB UK. (2021, April 20). Digital ad market proves resilient with 5% growth in 2020.https://www.iabuk.com/research/digital-ad-market-proves-resilient-5-growth-2020Juniper Research. (2023). Quantifying the cost of ad fraud: 2023-2028.https://fraudblocker.com/wp-content/uploads/2023/09/Ad-Fraud-Whitepaper_Juniper-Research.pdfMozilla Foundation. (2024, April 16). Full disclosure: Stress testing tech platforms' ad repositories.https://www.mozillafoundation.org/en/research/library/full-disclosure-stress-testing-tech-platforms-ad-repositories/Richet, J. L. (2022). How cybercriminal communities grow and change: An investigation of ad-fraud communities. Technological Forecasting and Social Change, 174, 121282. DOI: 10.1016/j.techfore.2021.121282
Science, Innovation and Technology Committee. (2025). Social media, misinformation and harmful algorithms: Second report of session 2024-25 (HC 441). House of Commons.https://publications.parliament.uk/pa/cm5901/cmselect/cmsctech/441/report.htmlUnited Nations. (2024). United Nations global principles for information integrity: Recommendations for multi-stakeholder action. United Nations.https://digitallibrary.un.org/record/4052524?v=pdf

4. Causes and impacts of fraudulent advertising

Q2: Do you have any comments on Ofcom's assessment of the causes and impacts of fraudulent advertising? Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.

CAN broadly agrees with Ofcom's assessment, including its recognition of the financial and emotional consequences for victims and the wider effects on businesses and trust. We suggest, however, that three additional dimensions deserve greater emphasis.

First, the analysis should more clearly recognise the economic infrastructure supporting fraudulent advertising and its relationship with organised crime. Fraudulent advertising should not be understood only in terms of individual fraudsters paying platforms to reach potential victims. Evidence has identified links between sophisticated advertising fraud and organised criminal activity, while the UK Stop Ad Funded Crime (UKSAFC) initiative has drawn particular attention to the wider problem of advertising revenues funding illegitimate and criminal actors (House of Lords Select Committee on Communications, 2018; UKSAFC, n.d.). The opacity of the wider digital advertising supply chain can additionally make it difficult to establish where advertising revenues ultimately flow and which actors financially benefit (Science, Innovation and Technology Committee, 2025).

The relevant policy question is therefore not only "how did this fraudulent advertisement reach a consumer?" but also "who ultimately benefits financially, and what visibility exists across the transaction and wider supply chain?"

This makes transparency over payment relationships, beneficial ownership, advertising intermediaries and supply-chain participants particularly important. Account verification should form part of a broader Know Your Customer/Know Your Business approach to the digital advertising ecosystem. This is consistent with the Science, Innovation and Technology Committee's (2025) recommendation that KYC checks should apply to participants in the programmatic advertising supply chain.

Second, CAN encourages Ofcom to recognise the market-wide consequences of declining trust. Fraudulent advertising damages not only individual victims but confidence in legitimate online advertising and businesses. Which? (2026) found that scam experience can lead consumers to favour familiar companies and withdraw from less familiar online businesses, potentially disadvantaging smaller firms and inhibiting

innovation. Fraudulent advertising therefore produces wider competition and economic consequences as well as direct financial losses.

Third, the speed and accessibility of generative AI are changing both the scale and sophistication of fraud. Generative AI can lower barriers to producing convincing synthetic text, images, audio and video, including deepfakes and impersonations, enabling fraudulent content to be produced and deployed at greater scale and sophistication (Home Office, 2026a, 2026b). These capabilities are particularly relevant to fraudulent advertising, where synthetic endorsements, impersonation and rapidly produced creative content can increase the credibility and reach of fraudulent campaigns.

This development also strengthens the case for advertiser verification, traceability and transparency. As the content of fraudulent advertisements becomes easier to generate and more difficult to distinguish from legitimate material, effective prevention will increasingly depend not only on assessing the content of an advertisement, but also on establishing who is behind it, on whose behalf they are acting, and whether the advertiser and associated transactions can be reliably traced. Robust KYC/KYB processes and auditable advertising records therefore become increasingly important complements to content-based fraud detection.

CAN therefore welcomes Ofcom's proposed testing of advertisement-generation tools, but stresses that the fraud-indicator framework and Codes will need to be capable of rapid updating as techniques evolve.

There is also an important timing issue. Which? has repeatedly highlighted the consumer-protection gap created by the current implementation timetable, with the statutory protections not expected to be enforceable until 2027 at the earliest. Given the speed at which AI-enabled fraud is developing, CAN encourages Ofcom to implement and enforce the Codes as soon as practicable and to encourage providers to adopt the proposed safeguards before the formal compliance deadline.

References

Home Office. (2026a). Fraud strategy 2026 to 2029: Disrupting crime, supporting economic resilience and delivering justice. HM Government.https://www.gov.uk/government/publications/fraud-strategy-2026-to-2029/fraud-strategy-2026-to-2029-disrupting-crime-supporting-economic-resilience-and-delivering-justice-accessibleHome Office. (2026b). National Assessment Centre fraud assessment 2025. HM Government.https://www.gov.uk/government/publications/national-assessment-centre-fraud-assessment-2025/national-assessment-centre-fraud-assessment-2025House of Lords Select Committee on Communications. (2018). UK advertising in a digital age (HL Paper 116). House of Lords.https://publications.parliament.uk/pa/ld201719/ldselect/ldcomuni/116/11602.htmScience, Innovation and Technology Committee. (2025). Social media, misinformation and harmful algorithms: Second report of session 2024-25 (HC 441). House of Commons.https://publications.parliament.uk/pa/cm5901/cmselect/cmsctech/441/report.htmlUK Stop Ad Funded Crime. (n.d.). Advertising fraud. UKSAFC.https://uksafc.org/advertising_fraudWhich? (2026, June 15). Which? responds to UK Finance's 2026 fraud report.https://www.which.co.uk/policy-and-insight/article/which-responds-to-uk-finances-2026-fraud-report-a59ah9n36VKB

Q3: Do you agree with the examples of risky characteristics we have provided? Please provide any arguments and supporting evidence.

CAN broadly agrees with Ofcom's proposed risky characteristics, but recommends that the Codes make clear that these are non-exhaustive, regularly updated and applied at both individual-advertisement and network level. Updates should draw on emerging intelligence from regulators, law enforcement, civil society, advertisers and independent researchers.

In particular, CAN recommends that services should be expected to assess behavioural, transactional and network-level indicators, rather than relying predominantly on characteristics of advertising content. Relevant indicators may include rapid changes in advertising volume or spend; repeated changes to payment instruments, account administrators, domains or destination URLs; multiple apparently unrelated advertising accounts sharing infrastructure or payment information; repeated creation of new accounts following

enforcement action; unusual geographical discrepancies between the advertiser, payment source and target audience; rapid switching between domains or landing pages; cloaking; and connections to previously identified fraudulent actors. This is particularly important because sophisticated fraudulent activity can involve multiple accounts, identities, domains and other digital infrastructure, making relationships between apparently separate activities relevant to detection (Home Office, 2026).

This requires services to be capable of identifying relationships across advertising accounts, organisations, domains, payment mechanisms and other relevant commercial actors, rather than assessing each account in isolation. CAN therefore recommends that the Codes require services to maintain sufficient information and audit trails to enable these relationships to be identified where fraud indicators arise. This should complement appropriate KYC/KYB checks by allowing services to identify not only who opened an advertising account, but whether that account forms part of a wider pattern of potentially fraudulent activity.

However, greater traceability should not be interpreted as requiring indiscriminate collection or disclosure of impression-level personal data. Transparency and fraud-prevention measures should be designed consistently with data-protection principles, including data minimisation and purpose limitation. The EU Digital Services Act provides a useful precedent: its advertising transparency framework requires disclosure of information concerning advertisers, payers, targeting and advertising reach, while expressly excluding recipients' personal data from public advertising repositories and providing separate mechanisms for regulatory and researcher access to platform data (European Parliament & Council of the European Union, 2022; EDPB, 2026). CAN therefore recommends a similarly proportionate approach, providing sufficient visibility to establish the provenance, relationships and financial flows associated with advertising activity without unnecessarily increasing surveillance of individual users.

References

European Parliament and Council of the European Union. (2022). Regulation (EU) 2022/2065 of 19 October 2022 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Act). Official Journal of the European Union, L 277, 1-102.https://eur-lex.europa.eu/eli/reg/2022/2065/oj?eliuri=eli:reg:2022:2065:oj&locale=enEuropean Data Protection Board. (2026). Guidelines 3/2025 on the interplay between the DSA and the GDPR (Version 2.0). https://www.edpb.europa.eu/documents/guideline/guidelines-32025-on-the-interplay-between-the-dsa-and-the-gdpr_enHome Office. (2026b). National Assessment Centre fraud assessment 2025. HM Government.https://www.gov.uk/government/publications/national-assessment-centre-fraud-assessment-2025/national-assessment-centre-fraud-assessment-2025

5. Our approach to developing Codes measures

Q4: Do you agree with our proposed approach? Please provide any arguments and supporting evidence.

CAN supports Ofcom's layered, safety-by-design approach and particularly welcomes the combination of fraud-indicator assessments, advertiser verification, account-security measures, AI-tool testing, reporting mechanisms, advertising libraries and forthcoming proposals for proactive detection.

However, CAN recommends strengthening the approach in three respects.

First, transparency should operate as a cross-cutting requirement throughout the Codes. Detection, reporting and enforcement are considerably less effective where regulators, advertisers and appropriately authorised independent experts cannot establish who purchased an advertisement, how it was distributed, what entities participated in the transaction and where money flowed.

Second, Ofcom should ensure that compliance is assessed in terms of outcomes as well as processes. The existence of policies, verification procedures or automated detection systems does not by itself demonstrate that they are effective. Providers should therefore monitor and evidence the effectiveness of their interventions, including rates of repeat offending, speed of removal, re-entry following bans and other

appropriate outcome measures. Independent audit should play a role in testing these claims, consistent with emerging regulatory approaches that use independent audit to assess the effectiveness of platform risk-mitigation measures (European Commission, 2024).

Third, the Codes should be embedded within a coordinated regulatory response. Fraud crosses the boundaries between online safety, financial regulation, advertising regulation, data protection, competition policy and criminal enforcement. CAN recommends structured cooperation and intelligence-sharing between Ofcom, the FCA, ASA, CMA, ICO, relevant law-enforcement bodies and government departments.

The Online Advertising Taskforce could provide a useful mechanism for broader coordination. Its remit already includes improving transparency and accountability in the online advertising supply chain, and its 2026 work programme has placed renewed emphasis on transparency and fraudulent advertising (Department for Culture, Media and Sport [DCMS], 2026). CAN recommends strengthening this role and ensuring meaningful representation from civil society and independent academic experts alongside industry.

References

Department for Culture, Media and Sport. (2026, March 17). Online Advertising Taskforce - progress report 2025.https://www.gov.uk/government/publications/online-advertising-taskforce-progress-report-2025/online-advertising-taskforce-progress-report-2025European Commission. (2024). Commission Delegated Regulation (EU) 2024/436 of 20 October 2023 supplementing Regulation (EU) 2022/2065 by laying down rules on the performance of audits for very large online platforms and very large online search engines. Official Journal of the European Union.https://digital-strategy.ec.europa.eu/en/library/delegated-regulation-independent-audits-under-digital-services-act

6. Combined impact assessment

Q5: Do you consider the overall burden on the service providers in scope of our proposed measures to be proportionate? Please provide any arguments and supporting evidence.

Yes. CAN considers the overall burden proportionate to the scale of the harm, the size and resources of the services in scope, and the central role that their advertising systems play in facilitating access to UK consumers.

The relevant comparison is not between the cost of implementing safeguards and zero cost, but between those costs and the substantial economic, social and human costs created by fraud, together with the commercial benefits platforms derive from operating advertising systems at scale.

Moreover, many of the proposed measures - advertiser verification, account security, fraud detection, audit trails and effective governance - reflect established principles of risk management in sectors handling significant financial transactions and associated fraud risks.

CAN would caution against weakening measures simply because implementation involves significant expenditure by providers. Where business models generate substantial revenues through highly automated advertising systems, the costs of making those systems demonstrably safer and more accountable should properly form part of the cost of operating them.

Volume 2: Risk, governance and control

2. Advertising intermediaries

Q6: Do you agree with our proposal? Please provide any arguments and supporting evidence.

No response

Q7: We have included two illustrative examples of when and how this measure may be applied, and what 'all reasonable endeavours' might look like. Do you have any comments on these examples, and do you have any additional examples of how providers could work with or require intermediaries to implement safety measures in circumstances where they have insufficient control? Please provide any arguments and supporting evidence.

No response

3. Fraud indicator assessment

Q8: Do you agree with our proposal? Please provide any arguments and supporting evidence.

No response

Q9: Do you think there are other information sources providers should consider in order to understand how fraudulent advertising manifests on their service? If so, what information and why would they need to consider it?

No response

4. Governance and accountability

Q10: Do you agree with our proposals? Please confirm which proposed measure your views relate to and provide any arguments and supporting evidence.

No response

5. Testing advertisement generation tools

Q11: Do you agree with our proposal? Please provide any arguments and supporting evidence.

No response

Volume 3: Ensuring account integrity

2. Account checks and actions

Q12: Do you agree with our proposal? Please provide any arguments and supporting evidence. Where your feedback relates to a specific check we are proposing providers should carry out, please make this clear. These are :

Yes. CAN supports Ofcom's proposed account checks and actions, particularly the verification of advertising account holders, measures to prevent banned actors from re-entering advertising systems, and repeat checks where relevant circumstances change.

These proposals are directly relevant to CAN's longstanding concern with accountability and traceability within the digital advertising supply chain. In particular, CAN encourages Ofcom to consider advertiser verification within a proportionate Know Your Customer/Know Your Business (KYC/KYB) framework. The potential role of KYC checks within the digital advertising ecosystem has also been raised in recent parliamentary scrutiny of the transparency and integrity of the programmatic advertising supply chain (Science, Innovation and Technology Committee, 2025). Verification should establish a credible relationship between the account holder and the individual or organisation being advertised and, for higher-risk accounts or activities, could include verification of organisational identity and, where proportionate, beneficial ownership.

CAN also supports measures to identify links between new accounts and previously banned actors. Such checks are important if account-level enforcement is to prevent fraudulent actors simply re-entering advertising systems through new or linked accounts. Importantly, verification should not be treated solely as a one-off onboarding exercise. Accounts can change ownership or administrators and legitimate accounts can be compromised. Risk-based repeat verification following material changes can therefore form an important part of an effective preventative approach.

More broadly, these measures should be supported by sufficient record-keeping and transparency to make advertising actors and transactions traceable and auditable. This connects account integrity directly with the wider transparency measures discussed in our response to Volume 1.

References

Science, Innovation and Technology Committee. (2025). Social media, misinformation and harmful algorithms: Second report of session 2024-25 (HC 441). House of Commons.https://publications.parliament.uk/pa/cm5901/cmselect/cmsctech/441/report.html

Q12.A: verification that advertising account holders work for, or on behalf of, the individual or organisation they are advertising

No response

Q12.B: checks and actions to prevent banned advertising account holders returning

No response

Q12.C: checks for accounts with indicators that there is a material risk they will post fraudulent advertising so that restrictions can be applied to them

No response

Q12.D: repeat checks where there are relevant changes identified on an account.

No response

Q13: Are you aware of any other account checks and actions providers could do to protect users from fraudulent advertising? Please provide any arguments and supporting evidence.

Yes. In addition to the measures proposed by Ofcom, CAN recommends that higher-risk advertising activity should trigger enhanced verification and traceability checks. These could include, where proportionate, verification of organisational identity and beneficial ownership; checks for relationships with previously banned actors; and examination of connections between accounts, domains, payment mechanisms and other relevant infrastructure.

These measures should be supported by sufficient record-keeping to enable relevant relationships between advertising accounts, organisations, intermediaries, domains and payment mechanisms to be traced where suspected fraud is identified. This reflects CAN's wider position that transparency and traceability are themselves important fraud-prevention measures, rather than simply mechanisms for investigating fraud after it has occurred.

3. Preventing fraudulent financial services advertising

Q14: Do you agree with our proposal? Please provide any arguments and supporting evidence.

No response

4. Countering account takeover

Q15: Do you agree with our proposals? Please confirm which proposed measure your views relate to and provide any arguments and supporting evidence.

No response

Q16: Do you have any evidence about account takeover that could inform our assessment, including how frequently it occurs or its impact?

No response

5. Advertising bans

Q17: Do you agree with our proposal? Please provide any arguments and supporting evidence.

No response

Q18: Are you aware of any additional exceptional circumstances in which it may be proportionate for providers to reverse advertising bans?

No response

6. Account appeals

Q19: Do you agree with our proposals? Please confirm which proposed measure your views relate to and provide any arguments and supporting evidence.

No response

Volume 4: Moderation

2. Advertising moderation

Q20: Do you agree with our proposals? Please confirm which proposed measure your views relate to and provide any arguments and supporting evidence.

No response

3. Terms of service and publicly available statements

Q21: Do you agree with our proposals? Please confirm which proposed measure your views relate to and provide any arguments and supporting evidence.

No response

4. Advertising complaints (including DRC for trusted flaggers)

Q22: Do you agree with our proposals? Please confirm which proposed measure your views relate to and provide any arguments and supporting evidence.

No response

5. Ad libraries

Q23: Do you agree with our proposal? Please provide any arguments and supporting evidence.

No response

Q24: Do you agree with the principles, functionalities and information categories which we have included in the proposed measure? Please explain your reasoning and, if possible, provide supporting evidence.

No response

Q25: Do you have any evidence or insights on the process of building an ad library from scratch or adjusting an ad library to align with the proposed measure, and how long that process would take?

No response

Additional questions

Q26: Do you agree with our Equality Impact Assessment? Please provide any arguments and supporting evidence.

No response

Q27: Do you agree with our Welsh language assessment? Please provide any arguments and supporting evidence.

No response

Q28: Do you agree with our proposals? Please provide any arguments and supporting evidence.

No response