Consultation response

Field	Value
Responder	IAB UK
Responder Type	organisation
Org Role	Head of Policy and Public Affairs
Org Type	Other
Other Type	Trade Association

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?

IAB UK welcomes Ofcom's recognition that an effective response to fraudulent advertising must reflect how digital advertising is bought, sold, served and measured in practice. However, while Ofcom's distinction between owned-and-operated, open-display and hybrid supply chains is a useful starting point, this does not fully capture the range of third-party relationships that exist within digital advertising.

The ecosystem should not be understood as a single linear chain in which all participants hold the same information or take the same interventions. Digital advertising comprises a number of actors who play different functions in the ecosystem and therefore have different information available to them. There are also many different formats and commercial arrangements. In some cases, a service provider will directly onboard an advertiser, receive payment, review an advertisement, control targeting and can prevent delivery if needed. In other cases, advertisements are placed through agencies, technology providers, resellers and/or automated supply chains. It is also very common for certain functions within the digital advertising supply chain that are not directly related to the placement of an ad - such as brand safety, measurement and verification - to be undertaken by third parties. The visibility and control exercised by individual actors for each of these functions differ materially.

For example, an agency may act for a verified advertiser; a demand-side platform (DSP) may receive buying instructions but not control the final delivery of the advert; a supply-side platform (SSP) may manage the inventory in which advertising can be sold but not possess the advertiser's full identity record; an ad server may execute delivery but not determine advertiser eligibility; and a verification provider may assess a defined attribute - such a brand safety metrics - without holding the authority to remove an advertisement.

The consultation documents also fail to recognise some of the more complex hybrid models that exist within the ecosystem. For example, reseller arrangements where a third-party company buys advertising space from a publisher and sells it to advertisers on their behalf.

The differences in these types of relationships have a significant implication on the application of the Codes. A requirement should be directed to the party with sufficient practical control and reliable information to perform it. We also encourage Ofcom to more clearly distinguish between:

- Direct advertisers and advertisers acting through agencies, authorised representatives, franchises, group companies and/or resellers.
- Publishers or service providers who control their inventory, and those that work with agencies, SSPs, or resellers.

- Services with full pre-publication review and those who use third parties and have more limited visibility or technical ability to intervene.
- Intermediaries involved directly in buying, selling or serving advertising and third parties providing supporting services such as measurement, verification or security.

While this section of the consultation does reference some of the existing industry transparency standards that can support supply chain accountability, it does not recognise the full suite of available cross-industry standards, including all IAB Tech Lab standards (like ads.txt and sellers.json), the IAB Gold Standard, independent third-party verification vendors like IAS and DoubleVerify, and external trust and safety providers like the Trustworthy Accountability Group (TAG) and The Media Trust. While none of these standards or third-party tools can be treated as comprehensive fraud prevention tools, they are an established part of how the online advertising ecosystem currently works and should be referenced more explicitly.

Finally, Ofcom's proposals only apply to paid-for advertising content on categorised services where the provider of that service is directly paid for the advert and controls its placement. However, the distinction between "paid-for" advertising and other types is not so clearly bounded in practice - for example, creator marketing and affiliate advertising would fall out of its scope. Ofcom assumes that providers will be able to apply this complex legal definition effectively and at scale and make real-time judgements about which content rules are applicable to a particular advertisement.

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.

IAB UK agrees that fraudulent advertising can cause substantial financial, emotional and practical harm to consumers, as well as harming legitimate businesses and trust in advertising funded services. Criminal actors can exploit the scale, speed, targeting capability and cross-border nature of online advertising, and may adapt rapidly following enforcement action.

We encourage Ofcom to give particular weight to the following features of the problem:

- Fraud is adaptive. Bad actors may alter creative, accounts, payment instruments, URLs, supply paths or jurisdictions after a control is introduced. The Codes should support continuous learning and adaptation rather than prescribe static procedures.
- Fraud is often multi-stage. The advertisement visible to consumers may be only one element of a wider operation involving impersonation, social engineering, cloned domains, account compromise or off-service activity. It is not reasonable or practical to expect providers to monitor activity that takes place beyond the content of the advert itself. Effective intervention will therefore require cooperation among platforms, advertisers, financial institutions, law enforcement and relevant regulators to remove the fraudulent activity at source.
- While helpful, distinct attributes of an advert are not in and of themselves proof of fraud. Certain categories, formats, languages, targeting choices, claims or use of urgency can be relevant risk signals in context, but should not be isolated and treated as evidence in itself that an advertisement is fraudulent.
- False positives have real consequences. Incorrect removal of ads, restrictions or account bans can deny legitimate businesses access to customers, disrupt campaigns, and damage brands. This is particularly relevant for small businesses, agencies serving multiple clients, regulated firms and businesses using legitimate but unconventional commercial structures.
- A distinction is needed between fraud and non-fraud non-compliance. Misleading, harmful or non-compliant advertising may be within the ASA, FCA, CMA or other regimes without necessarily meeting the statutory threshold for a fraudulent advertisement under the OSA. The Codes should not collapse these categories.

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

IAB UK supports Ofcom's broad approach where 'risky' characteristics are treated as contextual signals that may trigger further checks or review, rather than as conclusive evidence of fraud.
The final Codes should state consistently that risky characteristics or signals are not in and of themselves a definite indictor of fraud or a substitute for the statutory "reasonable grounds to infer" threshold. They should be assessed in combination. This is especially important where signals may correlate with legitimate businesses, including new entrants, SMEs, overseas advertisers lawfully targeting UK consumers, or legitimate AI-assisted creative.
At the same time, keeping in mind that an in-scope provider need only take proportionate steps aligned with its risk assessments, they should not be required to conduct further inquiries where they have determined, even on the basis of relatively limited information, that an advertising account is likely to be fraudulent.
Providers should also be permitted to calibrate signals against their own service-specific experience. A signal that is strongly predictive of fraud on one service or in one format may be weak or non-predictive in another.
Ofcom should not create a fixed or exhaustive list that becomes an evasion guide for criminal actors or unintentionally entrenches over-zealous enforcement.

5. Our approach to developing Codes measures

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

IAB UK supports the objective of Codes that gives providers of in-scope services practical and proportionate measures for complying with their duties. We welcome the recognition that providers can use alternative measures where they can demonstrate compliance.
We recommend three refinements:
- First, the Codes should be explicitly outcomes focused. They should establish the safeguards and results that Category 1 and 2A services need to achieve, while enabling different services to deploy equivalent or more effective methods - particularly where providers already have the technology in place to do so. The same prescriptive workflow will not necessarily be appropriate across all advertising formats and service designs.
- Second, the Codes should apply a stronger control-based approach. Measures concerning onboarding, verification, moderation, reporting, removal and disclosure should reflect the provider's actual ability to perform the action. This is especially important where placement involves intermediaries.
- Third, Ofcom should include an ongoing review mechanism. The final Codes should be supported by ongoing engagement with industry, regulators and civil society to identify emerging fraud types, improve interoperability and address unintended consequences. Where a measure imposes significant operational change, Ofcom should allow realistic implementation periods and consider phased introduction or piloting.

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.

IAB UK supports proportionate investment by providers of in-scope services to combat fraudulent advertising. However, the cumulative burden of the proposed measures may be substantial, particularly where a provider must introduce or materially expand account verification, repeat checks, moderation systems, tracking, record retention, appeals, trusted-flagger arrangements, ad libraries and public APIs at the same time.
The burden should be assessed cumulatively, not measure by measure. The operational impact will vary by service design and by the extent to which the provider controls advertiser onboarding, account data, destination URLs, delivery and enforcement.
Ofcom also does not consider that the burden of many of these measures will in practice fall not just on the category 1 and 2A services, but the whole digital advertising ecosystem including advertisers, intermediaries and SMEs who rely on the services in scope to deliver advertising. This should be acknowledged and

appreciated by Ofcom.

Volume 2: Risk, governance and control

2. Advertising intermediaries

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

IAB UK welcomes Ofcom's recognition that a Category 1 or 2A service may lack sufficient control to implement a recommended measure in full, and that cooperation with advertising intermediaries may be relevant. The inclusion of the proposed measure K1 is preferable to an approach that assumes every provider has identical visibility and control.

However, it requires amendment. As drafted, K1 states that a provider that cannot implement a measure, wholly or partly, should use "all reasonable endeavours" to implement a version "as similar to the measure as possible". It states that this should include, where applicable, requiring or working with intermediaries to implement a version of the measure.

It must be noted that statutory duties under s.38(1) and s.39(1) of the Online Saftey Act are fundamentally built on individual corporate accountability, not requiring supervision or scrutiny of intermediaries' backend operations by services. The Codes do not provide examples of how Ofcom would assess if "all reasonable endeavours" have been used, which creates confusion for providers of in-scope services in understanding how to enact this in practice and provides Ofcom with too much license to decide what is and is not acceptable. This could ultimately lead to significant burdens being placed on services working with a wide range of external partners, or for Category 1 or 2A services to cease working with intermediaries due to the legal complexities - which could have knock-on impacts for the wider advertising ecosystem and the legitimate parts of the supply chain who work with these intermediaries.

We recommend that Ofcom amend K1 to make clear that:

- The relevant test is whether a Category 1 or 2A service has taken reasonable and proportionate steps to mitigate the relevant risk considering its actual legal, contractual, technical and operational control, i.e. the requirement of a service provider to use "reasonable endeavours" would be deemed fully satisfied upon the negotiation and enforcement of robust and binding contractual commitments with its direct partners.
- A Category 1 or 2A service should not be expected to require an intermediary to perform an action where the intermediary in question lacks access to the relevant data, the authority to act, a lawful basis for processing or sharing information, or a realistic technical ability to implement the measure.
- "As similar as possible" should be replaced with an outcome-focused standard, for example: "a measure reasonably designed to achieve an equivalent level of protection against the relevant risk, having regard to the provider's degree of control".
- Written records should be proportionate, focused on material decisions and retained in a form that protects confidential commercial information, security-sensitive details and personal data.
- The Code should recognise that an advertising intermediary is not a homogeneous category. Different intermediaries perform different functions and will have different information and intervention points.

We would also recommend that Ofcom publishes a functional mapping of intermediary types against relevant Code measures, information held, intervention capability and associated fraud risks. Clarity on Ofcom's expectations in this area is critical as it will ensure that third party actors understand and prepare for the activity that providers may reasonably ask them to undertake in support of compliance.

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.

The examples provided are useful to show the potential real-world application of 'all reasonable endeavours'. However, consistent with our answer above, we would ask Ofcom to clarify:

- What 'requiring' means in practice (e.g. contractually,). Examples 2.1 and 2.2 confirm that the statutory expectations of "requiring" and "working with" intermediaries are fully met through direct contractual terms.
- How these would work in practice in instances where there are multiple intermediaries working across the same issue, or in instances where intermediaries do not have all the information in place on their own - for example in example 2.1, where it says arrangements should be put in place to ensure the provider has visibility of all paid-for ads, this would not just fall on the advertisers, or demand-side platforms, but on that information being passed consistently across the chain.
- Who should be accountable in instances where multiple intermediaries are involved in measures.

Both examples would be strengthened by referencing the existing transparency standards (Ads.txt, Sellers.json, DemandChain Object, and Buyers.json) and how they interrelate to one another as concrete mechanisms through which "reasonable endeavours" can be delivered. This would be consistent with wider initiatives across the online advertising ecosystem to encourage adoption of these standards, such as the IAB Gold Standard and the Working Group that IAB UK is co-chairing with the Home Office and DCMS on ad fraud and standards.

Finally, Ofcom's guidance must offer the operational latitude needed to leverage and refine existing user-safety and fraud-prevention systems. Formally acknowledging these prior technology investments through a flexible, outcomes-based approach will yield faster, more robust security upgrades without creating administrative hurdles.

3. Fraud indicator assessment

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

IAB UK supports a structured and evidence-led fraud indicator assessment. The proposed approach appropriately identifies a broad set of potentially useful sources, including moderation outcomes, complaints, trusted flaggers, law-enforcement referrals, internal expertise, retrospective analysis, testing, research, audits and data-sharing arrangements.

We recommend the following clarifications.

- The assessment should be calibrated to the service's role, information and ability to act. It should not require providers to obtain information that is not already in their possession or reasonably accessible, cannot lawfully be shared, is commercially confidential, or is of uncertain provenance.
- The requirement to request information from a third party where the service is aware the third party holds applicable and relevant information should be qualified. Third parties should not be expected to disclose data contrary to legal, contractual, confidentiality, competition or security obligations.
- The term "material risk" should be applied consistently, with regard to both likelihood and severity. Providers should be able to use qualitative, quantitative or mixed analytical methods appropriate to their service.
- Signals should be tested for accuracy, bias and unintended consequences. A risk indicator may be valuable for prioritisation but insufficient for a fraud finding, restriction or ban.
- The Code should recognise the risk of adversarial adaptation. Overly detailed public disclosure of indicators or assessment methodologies can make it easier for fraudsters to avoid detection.
- Review triggers should capture material changes in risk, not routine operational changes that are unlikely to affect fraud exposure.
- The requested information must be strictly limited to what is reasonably necessary for the provider to execute the Fraud Indicator Assessment, which also aligns with the data minimisation principle under the UK GDPR.

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?

n/a

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.

n/a

5. Testing advertisement generation tools

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

IAB UK supports proportionate testing of advertisement-generation tools made available by Category 1 and 2A services. Tools that generate or materially modify advertising content should be designed and operated with appropriate safeguards against misuse - particularly to impersonate brands, public figures and institutions.

The proposal should be refined to ensure it is risk-based and technologically neutral, as well as distinguishing between a tool that is specifically made available for creating advertisements on a categorised service from a general-purpose functionality that may incidentally be used in producing advertising materials. We recommend that Ofcom also clarify that these measures apply exclusively to AI Generation tools (AGTs) operating within a regulated service, strictly respecting the statutory limits of s.38(7) and s.39(7) of the OSA which prohibit extending obligations beyond regulated services.

Some AGT providers already have thorough systems in place to test, log, and evaluate model performance. We would therefore clarification from Ofcom that - where these exist - these existing, model-level safety audits are sufficient to meet the goals of this measure.

Finally, there is a risk that imposing rigid mandates on native platform tools will inadvertently discourage companies from offering built-in ad-creation features. This market shift may drive advertisers toward unmonitored, third-party software that lacks platform-level safety controls, resulting in a less secure ecosystem overall.

To offset this risk, Ofcom should ensure that requirements applying to native AGTs are proportionate, outcomes-focused and recognise the robust testing and evaluation infrastructure that providers already have in place.

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 :

IAB UK supports proportionate but robust measures to help verify whether an advertiser has the authority to advertise on a categorised service; identify repeat offending of fraudulent characteristics; and apply appropriate restrictions where there is a material risk of fraudulent advertising. We agree with an approach to account verification that ensures that advertisers and categories that pose the highest harm to consumers facing the highest threshold of checks and strong takedown requirements. This mirrors other account verification checks that happen across the online advertising sector.

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

e have concerns that the verification checks outlined in the draft Codes are disproportionate to the risks identified, given that they will apply universally across all advertisers who use the providers' services -

regardless of the type of product/s that they are advertising or their level of advertising spend. This will mean that in practice providers will have to implement the same costly and burdensome verification checks on many legitimate advertisers who show no risk signals relating to fraud and who may not have the internal processes to provide the levels of verification being asked
The potential impact of this will be most acutely felt by SMEs, who cumulatively make up the vast bulk of advertising spend on some Category 1 or 2A services, but who each only spend small amounts. For example, the requirement for a provider verifying that an account holder works for, or on behalf of, an advertised party will be harder and more burdensome for an SME given that standard methods for how this could work in practice, like checking Companies House records, will not apply uniformly. This type of uniform account check could lead to these SMEs not being able to legitimately advertise on these services, which would limit their ability to reach legitimate customers and grow their businesses. Further, industry feedback highlights that regardless of a platform's scale, providers lack any practical mechanism to validate private, third-party legal or contractual relationships between account holders and advertised entities. Therefore, we urge Ofcom to revisit this requirement in the final Code.
In order to avoid this type of disproportionate outcome on the wider advertising ecosystem, we recommend that Ofcom should at the outset clarify that the proposed verification checks in the Codes serve as an indicative framework of best practices, rather than a rigid list of mandatory requirements. Both the scope and timing of the required verification checks should be designed to remain strictly proportionate to the identified level of risk. Ofcom should replace its universal approach with a tiered risk-based approach, acknowledging that different advertising categories (such as financial services) may require different levels of verification depending on the level of potential risks to the end user. In many cases, a lot of categorised services already adopt this type of risk based approach - from two-tier verification for smaller accounts up to FCA-style verification for financial service ads. This risk-based approach would also prevent Ofcom's approach from being overly prescriptive, and therefore easier for criminal actors to understand and adapt their behaviours to meet the requirements. It would allow the provider to use a range of reliable, proportionate assurance methods without specifying which one would help with this, which may include direct verification, agency authorisation, contractual and payment signals, corporate or regulatory records, account history, domain control, advertiser attestation, brand-authorisation evidence and relevant behavioural indicators. The appropriate combination will depend on the service and the risk.

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

We outline our views on this in the "advertising bans" section

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.

Some members have also highlighted that to avoid imposing disproportionate data-collection burdens on in-scope providers, compliance under H1.3(b) must be governed by a risk-based, proportionate standard rather than an expectation of exhaustive investigation. For example, if a service's initial assessment of basic signals indicates that an advertising account is highly likely to be fraudulent, the provider must have the operational latitude to immediately restrict or reject that entity. We urge Ofcom to clarify that providers are permitted to make definitive screening decisions without being forced to conduct secondary inquiries.

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.

n/a

3. Preventing fraudulent financial services advertising

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

IAB UK strongly supports effective action to prevent fraudulent financial services advertising, given the level of serious consumer harm associated with investment scams, impersonation, unauthorised promotions and other forms of financial fraud. We support the use of the FCA Financial Services Register and Warning List as important sources of information. This is something already used and well understood by categorised services. However, it is important that the final Codes avoids duplication with that regime by clarifying that providers may reasonably rely on for:

- An advertisement approved for section 21 FSMA purposes.
- An applicable exemption.
- An agency's authority to place an advertisement for a legitimate financial-services advertiser.

The final Codes should also avoid treating all financial-services advertising as fraudulent where it does not meet a provider's policy criteria. A provider may lawfully impose more restrictive advertising policies, but a distinction should be maintained between a breach of platform policy and a finding of fraudulent advertising for OSA purposes.

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.

IAB UK supports measures requiring appropriate account security, accessible reporting of suspected account takeover, prompt review, account protection and restoration of access to authorised users.

The Codes should remain neutral as to the particular security mechanism utilised. Appropriate controls will depend on the account's risk profile, user base and available technology. Providers should be able to use multi-factor authentication, risk-based authentication, administrator controls, device and session protections, anomaly detection, recovery safeguards or equivalent mechanisms.

We support the proposal that an account affected by a confirmed takeover should not continue to serve advertisements until authorised access has been restored and the provider is satisfied that the account no longer poses a risk. Providers should have flexibility to apply more targeted mitigations where a full pause is not necessary and where this can be done safely.

The references in the draft Codes to persons authorised to access an account should be reviewed for consistency, including the apparent cross-reference issues in H4.3 and H4.4. The final drafting should ensure that an authorised account user can report a takeover without being able to log into the compromised account, and that recovery routes are secure enough not to create a further account-takeover risk.

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

n/a

5. Advertising bans

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

IAB UK supports decisive action against persons who are repeatedly responsible for posting fraudulent advertisements. If implemented in a proportionate and effective way, bans are one way of reducing repeat offending and disruption caused by rapid account re-creation.

However, a person-level ban is a serious intervention and, at present, the Codes as written state that a single violation triggers a ban with no distinction as to whether this is an isolated incident or a result of repeat offending. This is particularly important given the difficulty in using risk-based signals alone to determine whether an advertisement is fraudulent or not. As stated previously, risky "characteristics" can often be associated with legitimate advertising and therefore a single violation ban could mean that accounts are then

having to be reinstated routinely if the ad which caused the ban is found to be non-fraudulent. This is practically an administrative heavy procedure to reverse, and so a degree of proportionality needs to be baked into the process with account bans seen as one measure in a suite of tools used to counter fraudulent advertising.
The measure also outlines a set of proposed steps that providers can use to prevent banned actors from returning to a categorised service, based on shared characteristics with the banned account like account name, registration details. While this may be somewhat effective against simple re-entry, it does not reflect the real-world practices of experienced and motivated criminal fraudsters who can set up a fresh legal entry with new registration details and payment information. Ofcom should look beyond characteristics relating to ID and to measures like IP verification to truly tackle re-entry into categorised services.
Finally, in cases where repeat offenders are identified, we would support more intelligence sharing across the advertising ecosystem (such as with DSPs and publishers) to minimise the potential of these criminal actors turning up in other parts of the supply chain.

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

In addition to successful appeals, relevant circumstances may include:
- Verified unauthorised access or account takeover.
- Mistaken identity or erroneous matching to a banned person.
- A finding that an agency, employee or service provider acted without the advertiser's knowledge or authority, where the advertiser has taken credible remedial steps.
- A material change in ownership, control or authorised administration accompanied by appropriate re-verification.
- New authoritative information from a regulator, law enforcement body or other reliable source that materially changes the basis for the decision.

Any reinstatement should be risk-assessed and may appropriately be accompanied by heightened monitoring or proportionate restrictions.

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.

IAB UK supports accessible, usable and prompt appeal systems for account-level decisions. They are important safeguards against erroneous restrictions and bans, especially for SMEs and agencies whose ability to reach customers may be materially affected by an enforcement decision.
The Codes should make clear that "promptly" is risk sensitive and should accommodate the complexity of an appeal. A straightforward identity or document error may be resolved quickly, while an appeal involving account takeover, cross-account linkage, an agency relationship or a financial services claim may require longer investigation.
Some members have asked for Ofcom to clarify that the scope of "appropriate action" following an appeal under J4 be strictly confined to in-service remedies. Regulatory intervention under this measure should be restricted to service-level adjustments such as reinstating or removing the specific account or advertisement in question, and must not extend to mandating financial compensation or damages, as the current text may suggest. Further, to avoid creating unintended legal precedents, we recommend that Ofcom's guidance should explicitly state that J4 is not designed to establish, support, or imply any civil liability for losses resulting from the suspension of advertising accounts or the removal of fraudulent content.

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.

IAB UK supports effective and proportionate moderation of suspected fraudulent advertisements which would allow providers to take swift, proportionate action where an advertisement is fraudulent or in breach of an applicable policy or contract.

We welcome the Codes' recognition that providers must balance speed and accuracy. However, there is a concern that this could easily tip over into the removal of legitimate advertising. This is a particular risk given the term "reason to suspect" which could be interpreted at requiring every risky signal or report of suspected fraudulent advertising. Ofcom should be explicit that providers are able to triage based on severity and likely harm, reach, confidence, source reliability and available evidence. Providers should also be able to apply a risk based approach to removal, with high-harm fraudulent advertising warranting immediate interruption, and lower-harm advertising requiring further review.

Finally, the definition of "fraudulent advertising proxy" in the Codes also requires caution. It should not be used to convert any policy breach into a fraud outcome. A proxy finding should remain limited to circumstances in which the provider has reason to suspect a relevant fraudulent advertisement, and the policy or contractual breach genuinely relates to the type of suspected fraud.

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.

IAB UK supports meaningful public transparency about the proactive technologies used to support compliance with the fraudulent-advertising duties.

However, the disclosure obligation should be framed at an appropriate level of generality. A requirement to explain "how [the technology] works" should not compel disclosure of technical rules, model features, vulnerabilities, data sources or other information that could enable bad actors to evade controls or compromise security. It should also protect trade secrets and sensitive information about third-party security tools.

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.

IAB UK supports accessible reporting channels for suspected fraudulent advertisements and effective consideration of substantiated complaints. Indeed many of the providers of Category 1 and 2A services already have well-established channels for this. We support dedicated reporting channels for the listed trusted flaggers, including the ASA. The ASA's Scam Ads Alerts system is well known as a successful route for flagging advertisements that are fraudulent and many of the services in scope already utilise its alerts.

We also recommend Ofcom revisits D5.2(c) for previously reinstated ads, due to the risks it poses to user safety. Industry feedback suggests that highly sophisticated threat actors routinely exploit dormant ad accounts which are profiles that are intentionally kept inactive or compliant at first, only to be activated for major fraud campaigns later. Because a malicious actor can successfully appeal a suspension during an account's compliant phase, restricting a platform's automated systems from re-evaluating that same account later leaves a security vulnerability that could be exploited.

5. Ad libraries

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

IAB UK supports the principle of proportionate advertising transparency and recognises that ad libraries can play a part in this by assisting users, regulators and brands in scrutinising the advertising that appears on

services, and reporting suspected fraudulent advertising after it has been seen.
However, we have concerns about the breadth and prescriptiveness of the proposed measure. The Code should distinguish information necessary to enable meaningful fraud-related scrutiny from information that creates privacy, security, and commercial confidentiality risks. At present, it is unclear why Ofcom believes that ad libraries will help with fraud prevention, and the efficacy of them compared with other measures outlined in the Code.
An ad library should also not be designed in a way that enables criminal actors to map detection responses, replicate campaigns, exploit targeting practices, scrape personal data, or reverse engineer a service's commercial systems. The final Codes should allow for appropriate redaction, aggregation, time delay between the advert going live and being uploaded, access controls (such as log-ins) and other safeguards like anonymisation or encryption measures.
in addition, mandating the data fields under E1.16(e), (f), and (g) imposes a technical and administrative burden on in-scope services without sufficient evidence that these inclusion of these data fields would materially increase user safety. In reality, these complex metrics are highly unlikely to be useful to, or utilised by, average UK users or provide additional benefits to expert flaggers. Therefore, we recommend that Ofcom revisit these requirements from the proposed ad libraries.

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.

We recommend the following amendments to the information categories and functionality:
- Advertiser and account identity. The current assessment of ad libraries does not adequately consider the commercial sensitives involved with publishing ads and associated information. The final Codes should permit redaction, aggregation or alternative identifiers where disclosure would create a material privacy risk, facilitate identity theft, or reveal confidential commercial information.
- Targeting information. The phrase "particular groups of UK users" used in the Codes is potentially very broad. Granular targeting attributes can reveal sensitive inferences, commercially confidential information or techniques that can be exploited by criminal. Ofcom should require a standardised summary of targeting parameters relevant to fraud prevention, rather than granular disclosure of audience construction, inferred attributes or precise targeting logic.
- Scope of advertising. At present the ad library would apply to all paid advertising found on in-scope services rather than a risk-based approach where only advertising in certain categories that are more sensitive to abuse by fraudsters is displayed. Ofcom does not explain why a universal approach is needed to help with fraud detection and preventing.

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?

Implementation time will depend materially on whether a service has an existing library; which data fields are already collected and quality-assured; whether data can be segregated for UK users; how account and advertiser information is structured; whether historic data is available; and what changes are required to build secure public search, reporting and API functions.
If Ofcom is to move forward with the ad libraries proposal, it should allow a phased implementation period which permits services to prioritise the fields most useful for fraud scrutiny, introduce new functionality in stages, and apply safeguards before opening public or automated access.

Additional questions

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

n/a

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

n/a

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

n/a