VERITAS

Response to Ofcom's Consultation

Fraudulent Advertising Codes of Practice

September 2026

Prepared by

[redacted]

Founder and Principal Consultant
VERITAS

Clarity Where It Counts.

Document Control

Document	Response to Ofcom's Fraudulent Advertising Codes of Practice consultation
Respondent	VERITAS
Author	[redacted]
Date	September 2026
Confidentiality	This response is not confidential and may be published.

Executive Summary

VERITAS welcomes Ofcom's proposals for Fraudulent Advertising Codes of Practice for Category 1 and Category 2A services. Fraudulent advertising is not merely a content moderation problem. It is a governance, financial crime and consumer protection problem that can cause severe financial loss, distress and loss of confidence in digital markets.

We support a risk based and outcomes focused framework that combines robust advertiser and account integrity controls with effective governance, monitoring, escalation and redress. The most effective regime will prevent fraudulent advertisers from gaining or regaining access, identify emerging risk quickly, remove harmful advertising at pace and use intelligence from complaints, payment activity and linked accounts to strengthen controls.

Our principal recommendation is that Ofcom should frame the Codes around demonstrable control effectiveness. Providers should not be able to rely on the existence of policies or automated tools alone. They should be able to evidence senior accountability, calibrated risk assessments, proportionate verification, detection performance, repeat offender controls, incident learning and meaningful reporting to users and regulators.

About VERITAS

VERITAS is an independent Governance, Risk and Compliance consultancy specialising in governance, financial crime, operational resilience, regulatory implementation and emerging technology risk. We help organisations translate regulatory expectations into practical governance and control frameworks that support innovation while protecting customers and maintaining trust.

VERITAS priority position

The Codes should require clear senior ownership, risk based account verification, linked account detection, repeat verification when risk changes, rapid suspension and review processes, continuous control testing, and transparent reporting of outcomes rather than activity alone.

1. Online advertising ecosystem

Is there any information or evidence that could enhance Ofcom's understanding of the online advertising ecosystem?

The ecosystem should be understood as a chain of interdependent actors rather than a single platform and advertiser relationship. Advertising agencies, affiliate networks, payment providers, domain registrars, identity verification providers, cloud infrastructure and lead generation businesses may all influence the risk profile of an advertisement.

Fraudsters exploit fragmentation. They may use legitimate business credentials, compromised accounts, synthetic identities, mule payment arrangements, cloaking tools and rapidly changing landing pages. A control framework that assesses only the advertisement presented at onboarding may miss the wider network and post approval changes.

Ofcom should encourage providers to combine account level, campaign level and network level intelligence. This should include linked payment instruments, devices, domains, administrators, beneficial owners, contact details, creative assets and behavioural patterns. Where appropriate and lawful, intelligence sharing across platforms and with financial institutions can materially improve prevention.

2. Causes and impacts of fraudulent advertising

Do you have comments on Ofcom's assessment of the causes and impacts? Has anything important been missed?

We agree that fraudulent advertising causes direct financial harm, emotional distress and wider loss of trust. The impact can be amplified where advertisements impersonate regulated firms, public figures, trusted brands or government services.

A further impact is the transfer of costs to other parts of the system. Banks, payment firms, law enforcement, consumer bodies and legitimate advertisers absorb investigation, reimbursement and remediation costs. Fraudulent advertising therefore creates externalities beyond the service on which the advertisement appears.

Ofcom should also recognise vulnerability created by urgency, financial pressure, bereavement, isolation, limited digital confidence and neurodivergence. Harm assessments should consider not only the average user but the foreseeable impact on users who may be more susceptible to persuasive design, impersonation or high pressure claims.

3. Risky characteristics

Do you agree with Ofcom's examples of risky characteristics?

Yes. Risk indicators should be treated cumulatively rather than as isolated red flags. A newly created account, unusual payment method, high risk product, rapid campaign scaling, frequent changes to destination URLs and use of public figure imagery may together indicate a materially higher risk even where no single factor is conclusive.

The Codes should avoid creating a static checklist that fraudsters can design around. Providers should maintain dynamic typologies informed by intelligence, complaints, enforcement outcomes and control testing. Risk models should be reviewed regularly and subjected to human challenge.

Additional characteristics may include mismatches between advertiser identity and domain ownership, unexplained geographic inconsistencies, use of recently registered domains, recycled or lightly altered creative content, unusual administrator access patterns and repeated association with previously restricted entities.

4. Proposed approach to the Codes

Do you agree with Ofcom's proposed approach?

We broadly agree with a risk based and proportionate approach. The Codes should be sufficiently clear to establish minimum expectations while allowing providers to adapt controls to their service design, scale and risk exposure.

Proportionality should not become a route to weak controls. Large services with sophisticated advertising systems and extensive data capabilities should be expected to deploy correspondingly sophisticated prevention and detection measures. Smaller services should still meet core governance and account integrity outcomes, with implementation proportionate to their size and complexity.

Ofcom should distinguish between procedural compliance and effective compliance. Evidence should include control performance, false negative and false positive analysis, time to action, recurrence rates, complaint trends and remediation outcomes.

5. Overall burden and proportionality

Is the overall burden on providers proportionate?

In principle, yes. The proposed measures address a serious and foreseeable harm and are targeted at services with substantial reach. The burden should be considered against the scale of consumer harm and the economic costs imposed on victims and other sectors.

Implementation can be made more proportionate through clear expectations, reusable evidence standards and alignment with existing financial crime, identity and cyber security controls. Ofcom should avoid unnecessary duplication where providers can demonstrate that an existing control achieves the required outcome.

We recommend phased implementation, clear transitional guidance and early supervisory engagement. However, measures addressing repeat offenders, compromised accounts and materially high risk advertisements should not be delayed where providers already have the technical capability to act.

6. Verification of authority to advertise

Comments on verification that account holders work for, or on behalf of, the person or organisation advertised?

We support this measure. Verification should establish both identity and authority. Confirming that an individual exists is not enough if they are not authorised to advertise for the named organisation.

Controls may include corporate registry checks, verified domain email, direct confirmation through independently sourced contact details, evidence of agency appointment and checks against regulated firm registers where relevant. High risk sectors should attract enhanced verification.

Providers should also address impersonation of individuals and public bodies. Verification evidence should be retained, refreshed and linked to change monitoring so that material changes in ownership, administrators, payment methods or advertised entities trigger review.

7. Preventing banned account holders from returning

Comments on checks and actions to prevent banned account holders returning?

This is essential. A ban that applies only to one account identifier is unlikely to be effective. Providers should use proportionate linked account analysis covering identity, beneficial ownership, payment methods, devices, domains, contact details, administrators and behavioural signals.

The process should include safeguards against unfairly restricting legitimate users who share infrastructure or business relationships. Decisions should be reviewable, evidence based and supported by clear escalation routes.

Providers should measure recidivism and report internally on the rate at which removed actors attempt to return, the methods used and the effectiveness of controls.

8. High risk account indicators and restrictions

Comments on checks for accounts presenting a material risk?

We support a tiered control model. Restrictions can include lower spending limits, delayed campaign activation, manual review, limits on rapid changes, additional verification and closer post publication monitoring.

Risk scores should not be treated as fully autonomous decisions without governance. Providers should document model ownership, validation, change control, bias considerations, override authority and performance monitoring.

Where risk is high and potential harm severe, precautionary restrictions are appropriate while review is completed. The time taken to review should be proportionate and should not leave high risk advertising live by default.

9. Repeat checks after relevant changes

Comments on repeat checks where relevant account changes are identified?

We strongly support event driven re-verification. Relevant triggers should include changes in ownership, administrators, payment methods, domains, advertised products, geography, campaign scale and unusual login behaviour.

Repeat checks should be risk based rather than purely periodic. A low risk, stable account may require less frequent intervention, while a material change should trigger immediate review.

Providers should prevent circumvention by ensuring that changes made through agencies, linked accounts or technical integrations are captured within the same monitoring framework.

10. Additional account checks and actions

Are there other checks and actions providers could take?

Providers should consider beneficial ownership verification for higher risk advertisers, validation of landing page ownership, monitoring for post approval content changes, payment risk signals, domain age and reputation checks, and confirmation of regulatory authorisation where claims relate to regulated products.

Behavioural controls are also important. Sudden increases in spend, rapid creation of multiple near identical campaigns, repeated rejected advertisements and unusual administrative access may indicate elevated risk.

Providers should maintain a structured enhanced due diligence process for high risk cases and a clear framework for suspension, investigation, reinstatement and permanent exclusion.

11. Moderation, reports and complaints

Further arguments and evidence on moderation, reporting, complaints and appeals?

User reports should be treated as intelligence, not merely individual service tickets. Providers should aggregate complaints to identify linked campaigns, advertisers, domains and emerging typologies.

Reporting routes should be easy to find and should include a specific fraudulent advertising category. Users should receive confirmation, a meaningful update and clear signposting to relevant support or reporting bodies where harm may have occurred.

Appeals are important for legitimate advertisers, but reinstatement should require documented review. Where an advertisement is restored, the reasons should be recorded and the decision should feed into quality assurance. Providers should also monitor reviewer consistency and error rates.

12. Fraudulent advertising judgements guidance

Do you agree with Ofcom's proposed guidance on making fraudulent advertising judgements?

We broadly agree. The guidance should support timely action where there are reasonable grounds to suspect fraud, while recognising that providers are not expected to determine criminal liability.

Judgements should consider the advertisement, destination, advertiser, account history and wider network together. A narrow review of the creative content may be insufficient where the fraud becomes apparent only through the landing page, payment journey or linked entities.

Ofcom should include worked examples covering impersonation, investment fraud, fake retail, subscription traps, lead generation and advertisements that change after approval. Examples should demonstrate how multiple weak signals can combine into a reasonable basis for action.

VERITAS Recommendations

1. Assign named senior accountability for fraudulent advertising risk and control effectiveness.

2. Require risk assessments to cover the full advertising ecosystem, including agencies, payment instruments, domains and linked accounts.

3. Verify both advertiser identity and authority to act for the advertised person or organisation.

4. Apply enhanced due diligence to high risk products, sectors and account behaviours.

5. Use network analysis to detect repeat offenders and linked accounts, with safeguards for legitimate users.

6. Trigger re-verification when material account, payment, domain or campaign changes occur.

7. Monitor post approval changes to advertisements and landing pages.

8. Treat complaints and reports as aggregated intelligence and provide meaningful user feedback.

9. Test controls continuously and report outcomes including recurrence, detection performance and time to action.

10. Provide worked examples and phased implementation guidance while maintaining urgent expectations for high risk harms.

Conclusion

Fraudulent advertising damages individuals, legitimate businesses and confidence in online services. Ofcom's proposed Codes are an important opportunity to establish a consistent minimum standard for prevention, detection and response.

The strongest framework will combine proportionate account integrity measures with clear governance, senior accountability, effective intelligence use and continuous assurance. Providers should be expected not merely to operate controls, but to demonstrate that those controls achieve meaningful reductions in harm.

VERITAS welcomes continued engagement with Ofcom as the Codes and associated guidance are finalised.

[redacted]

VERITAS

Clarity Where It Counts.