Dear Ofcom Online Safety Team,

tScheme welcomes Ofcom's proposed Fraudulent Advertising Codes of Practice and supports their emphasis on preventing fraudulent advertisers from obtaining or misusing advertising accounts.

tScheme is an independent trust-services scheme with experience developing assessable criteria and working with accredited assessment processes for digital identity and trust services. Our contribution to this consultation concerns how platforms can demonstrate that their advertiser checks and related controls are effective, consistent and capable of being reviewed.

We support the proposed account checks in Volume 3, particularly the requirement to verify that an advertising account holder works for, or acts on behalf of, the person or organisation being advertised. The practical challenge is to establish and maintain the complete chain of assurance. A platform may know that an account operator is a real person without knowing whether that person is currently authorised to advertise for a particular business. An agency may be authorised by a business while an individual using its account is no longer authorised by the agency. A sound initial check can also be undermined by account takeover or a subsequent change of administrator.

We recommend that Ofcom's final guidance ask platforms to define the assurance outcomes their checks must achieve and retain evidence sufficient to review those outcomes. At a minimum, this should cover:

- the identity of the account operator and the advertiser;
- the operator's authority to act for the advertiser, including each relevant intermediary;
- the source, scope and currency of that authority;
- controls that bind the assurance to the advertising account and protect it against takeover or unauthorised changes;
- triggers for renewed checks when relevant circumstances change; and
- the action taken when evidence fails, expires, conflicts or is challenged.

These are distinct questions. Neither an identity check nor a business-register lookup alone establishes that a person may place a particular advertisement. Likewise, successful assurance of an advertiser does not establish that an advertisement or commercial offer is lawful or truthful. The account controls must operate alongside Ofcom's proposed moderation, financial-services verification, reporting and appeals measures.

The UK Digital Verification Services Trust Framework provides an independently certifiable foundation for relevant identity and attribute services. Ofcom could recognise certified services as one way to support advertiser checks without prescribing a single technology or provider. Platforms would remain responsible for assessing the authority relationship, securing accounts and determining whether their controls meet the outcomes required by the code.

We also recommend that Ofcom distinguish clearly between **using an assured component** and **assurance of the end-to-end advertising process**. Independent assessment of that process could examine whether policies are applied consistently, evidence is reliable and current, intermediary responsibilities are clear, exceptions are controlled, and performance is monitored over time. This would give platforms a practical means of demonstrating the effectiveness of their systems while giving Ofcom more comparable evidence when assessing implementation.

Proportionate assessment criteria would be especially useful where multiple platforms, agencies and verification providers participate in the same advertising chain. They could support reuse of suitable evidence and reduce repeated checks for legitimate advertisers, while allowing stronger scrutiny where fraud indicators warrant it. Such criteria should also test accessibility, data minimisation, correction and appeal, so that controls do not unnecessarily exclude legitimate advertisers.

We have attached a tScheme Fraudulent Advertising Technical Annex to this email

We would welcome the opportunity to discuss the design of assessable outcomes and evidence requirements with Ofcom as it develops its final guidance. tScheme can contribute experience in translating trust and identity requirements into criteria capable of independent assessment, including the treatment of intermediaries, lifecycle changes and continuing assurance.

Please treat this email as tScheme's response to the consultation questions on account checks and actions, advertising intermediaries, governance and accountability, and proportionality. We would be pleased to provide a more detailed technical annex if helpful.

Yours faithfully

[redacted]

Web: www.tscheme.org

tScheme Ltd, Technical annex assessable assurance for fraudulent advertising controls

Submission by tScheme Ltd to Ofcom

Consultation: Fraudulent Advertising Codes of Practice, September 2026

Status: Recommendations for consideration; not a statement of existing code requirements

1. Purpose and scope

Ofcom's draft measures H1–H5 address advertiser account checks, financial-services verification, security, takeover and bans. Measures B1 and A1–A6 address risk assessment and governance; C1–C7, D1–D7 and E1 address moderation, complaints and ad libraries; F1 addresses testing of advert-generation tools. This annex proposes **assessable outcomes and evidence** for the account and creative-provenance controls. It does not propose that certification of a component certifies an advertiser or an advert.

The assurance chain is: **account operator → advertiser → authority to act → advertising account and campaign → published creative and destination**. A platform should define which entity performs each check when an agency or other intermediary is involved and retain evidence that the check remains effective over time.

The purpose of these controls is not only to improve platform assurance but also to reduce consumer exposure to fraudulent advertising, increase transparency and strengthen confidence in digital advertising ecosystems. Assurance mechanisms should ultimately support clearer and safer user experiences.

The level of assurance applied should be proportionate to the risk presented by the advertiser, advertising category, audience exposure and potential consumer harm.

2. Illustrative outcomes and evidence

Outcome to assess	Evidence an assessor could sample	Failure or change scenario
Identity and advertiser existence. The operator and the advertiser are identified to a proportionate confidence level.	Verification policy; source and result of checks; identity or attribute assertion with issuer, validity and assurance information; business-register cross-check where relevant; sample case records.	Stolen identity, dissolved company, mismatched trading name, reused document.
Authority to act. The operator's mandate is traced through the agency chain to the advertiser, with a defined scope and duration.	Mandate or authenticated vouch from an authoritative contact; role and delegated permissions; agency contract reference; source validation; expiry and revocation events.	Agency contract ends, employee leaves, one agency claims another brand, authority covers a different account.
Account binding and control. Verified persons and mandates are bound to account privileges, and sensitive changes require suitable authentication and review.	Account-role matrix; authentication configuration; change logs; approval records; takeover detection and incident samples.	Admin takeover, new payment method or landing domain, transfer to another account holder.
Continuing assurance. Checks are repeated on defined triggers, and restrictions apply while material uncertainty remains.	Trigger rules; monitoring metrics; recheck events; exception register; restrictions, reinstatement and appeal records.	Expired assertion, revoked mandate, new fraud signal or conflicting information. Other examples: Merger, acquisition, change of ownership, significant control change

Outcome to assess	Evidence an assessor could sample	Failure or change scenario
Advert and destination linkage. The creative, advertiser and destination reviewed before publication can be linked to the version actually served.	Campaign identifier; approved asset digest or version; final URL and redirect checks; publication and edit logs; ad-library record.	Creative substitution, redirect change, altered AI-generated image or video after approval.
Governance and assurance. Management can test whether controls work, including across intermediaries and excluded or appealed cases. Independent assessments, where used, should be undertaken by competent and impartial assessors operating under recognised assurance arrangements.	Risk assessment; control ownership; sampling plan; false-positive and false-negative analysis; incident learning; independent review findings and remedial action.	High pass rates despite known scams; controls applied inconsistently by agency or platform.

An assessment should test both design and operation: sample real account and advert records, trace decisions to source evidence, test negative and changed circumstances, and verify that appeals can correct errors. The evidence categories above are illustrative and should be scaled to risk and data-protection requirements.

3. Role of certified digital verification services

An independently certified DVS may supply reusable evidence of a person's identity or relevant attributes. The platform must still decide whether that person is authorised to represent the advertiser and to use the particular account. A trust-framework certificate applies to the **certified service and its specified scope**, not automatically to an advertiser, a campaign or the truth of its claims. The platform should record the assertion relied on, its provenance, validity, permitted use and outcome, while minimising retention of raw identity documents.

Where appropriate, platforms should be able to accept reusable digital identity or attribute credentials from trusted providers, reducing duplication while maintaining assurance and privacy protections.

4. C2PA and advert provenance

C2PA Content Credentials can cryptographically bind a provenance manifest to a media asset and record assertions about creation, edits and ingredients, including AI-related steps. For an image or video advert, a platform could validate the manifest at upload and after processing, associate the validated asset or rendition with a campaign identifier, and preserve a verifiable reference in its internal records and, where suitable, its ad library. An authenticated advertiser or agency identity assertion could be linked to the provenance record using the applicable identity profile and separately established mandate. The signer's identity, the advertiser's identity and the authority to act on behalf of the advertiser should be treated as separate assurance questions requiring independent evidence.

Illustrative pilot: for selected high-risk ad categories, accept C2PA-bearing creative; validate its content binding, signature, trust chain, revocation status and ingredient history; record the result and the exact approved version; check whether platform transformations preserve or reconstruct a valid provenance chain; and expose a clear, limited explanation to users and trusted flaggers. Measure manifest survival, validation failures, investigation time and false confidence caused by misleading displays.

C2PA is **supporting evidence, not a fraud verdict**. A valid manifest does not establish that an advertised investment is lawful, a product exists, a claim is accurate, the signer is authorised by the brand, or a landing page is safe. An absent manifest is not proof of fraud. Metadata may be stripped during distribution; a platform should evaluate recovery or an external manifest repository and retain its own version linkage. Text, dynamic creative, multiple renditions, redirects and post-publication edits require additional controls. A visible badge should say what was validated, by whom and for which asset version, without implying Ofcom endorsement.

5. Recommended wording for Ofcom's guidance

> Providers should be able to demonstrate how their checks establish and maintain the identity of the advertiser, the authority of each person or intermediary acting for it, and the binding of that authority to the advertising account. Where provenance credentials are used for advertising creative, providers should validate and preserve their linkage to the version served, while continuing to assess the advertiser, content and destination independently.
>
> Providers should be able to demonstrate measurable reductions in fraudulent advertiser activity, account compromise and repeat offending, together with evidence that controls remain effective as threat patterns evolve.
>
> Providers may draw on independently certified digital verification services, recognised trust frameworks and content-provenance standards as appropriate to their risk profile
>
> and recognised content-provenance standards as appropriate to their risks; neither is, by itself, proof that an advertisement is genuine.

Ofcom could convene a focused technical workshop with platforms, advertisers, intermediaries, DVS providers, assessors, consumer representatives and C2PA implementers to test these outcomes against real account and campaign workflows. tScheme would be willing to contribute technical criteria and illustrative assessment cases. Any commissioned work would be pursued through Ofcom's applicable procurement arrangements.

Findings from implementation and pilot activity should be periodically reviewed to identify emerging fraud patterns, control weaknesses and opportunities for improvement.

No single control can prevent all fraudulent advertising activity. Identity verification, authority validation, provenance records and account-security controls each address different risks and should be deployed as complementary measures within a wider fraud-prevention framework.

Assurance provides increased confidence rather than absolute certainty. Effective controls therefore require ongoing monitoring, investigation, complaint handling and enforcement activity.

tScheme Ltd, Technical annex assessable assurance for fraudulent advertising controls

Sources

- Ofcom, *Fraudulent Advertising Codes of Practice consultation*, 10 July 2026, including Volumes 2–4 and draft Codes: https://www.ofcom.org.uk/online-safety/online-fraud/consultation-fraudulent-advertising-code-of-practice
- Ofcom, *Fraudulent Advertising Codes Consultation response form*: https://www.ofcom.org.uk/draft-fraudulent-advertising-codes-response-form
- UK Government, *UK Digital Verification Services Trust Framework (1.0)*: https://www.gov.uk/government/publications/uk-digital-verification-services-trust-framework-1-0
- C2PA, *Content Credentials technical specification, version 2.4*: https://spec.c2pa.org/specifications/specifications/2.4/specs/ContentCredentials.html
- C2PA, *Human and Organizational Identity Recommendation, version 2.4*: https://spec.c2pa.org/specifications/specifications/2.4/identity/identity.html
- C2PA, *Security Considerations, version 2.4*: https://spec.c2pa.org/specifications/specifications/2.4/security/Security_Considerations.html