UK Finance

OSA Fraudulent Advertising Codes Consultation

September | 2026

Contents

Executive Summary 3
1. Context 6
Online Advertising Ecosystem 6
Causes and Impacts of Fraudulent Advertising 7
Approach to codes 8
Combined impact assessment 10
2. Risk, Governance, and Control 15
Advertising Intermediaries 15
Fraud Indicator Assessment 20
Governance and Accountability 24
Testing Advertisement Generation Tools 28
3. Ensuring Account Integrity 29
Account Checks and Actions 29
Preventing Fraudulent Financial Services Advertising 32
Countering Account Takeover 35
Advertising Bans 38
Account Appeals 39
4. Moderation 42
Advertising Moderation 43
Terms of Service and Publicly Available Statements 45
Advertising Complaints 46
Ad Libraries 47

Executive Summary

UK Finance is the collective voice for the banking and finance industry. Representing 300 firms, we are a centre of trust, expertise and collaboration at the heart of financial services, championing a thriving sector and building a better society.

UK Finance welcomes Ofcom's Fraudulent Advertising Code of Practice consultation and supports the introduction of stronger obligations on Online Services to identify, prevent and disrupt fraudulent advertising. The proposals represent an important step towards strengthening accountability within the online ecosystem and reducing the harm caused by fraud and scams facilitated through paid-for advertising.

Executive Summary

Fraudulent advertising remains a major enabler of economic crime. UK Finance's Annual Fraud Report 2026 shows that criminals stole £1.28 billion through payment fraud in 2025[1], with APP fraud losses increasing by 19% to £576.4 million. Most APP fraud originates outside the financial sector, with 66% beginning online and a further 17% through telecommunications networks. This demonstrates that Online Services are a critical intervention point for preventing harm before consumers are targeted.

To maximise the effectiveness of the Fraudulent Advertising Codes, Ofcom should move beyond high-level principles and establish a minimum operating model for in-scope services. This should include requirements for advertiser verification, pre-publication screening, ongoing monitoring, trusted-flagger escalation routes, repeat-offender controls, evidence preservation, and standardised outcome reporting. Success should be measured through outcomes, including reductions in fraudulent adverts, scam losses, repeat offenders, and service response times.

The minimum operating model should cover the full control lifecycle: advertiser onboarding and verification, pre-publication screening, continuous monitoring, trusted-flagger escalation, restriction or removal, evidence preservation, consumer notification and standardised outcome reporting. Providers should retain flexibility over implementation, but the minimum control outcomes should be clear, comparable and enforceable.

A key challenge is that Online Services and advertising intermediaries can derive revenue from advertising activity, including adverts later identified as fraudulent. Ofcom should therefore recognise these commercial incentives and establish clear,

[1] UK Finance Fraud Report 2026.pdf

enforceable expectations requiring providers to prevent, detect, and remove fraudulent advertising even where doing so may conflict with short-term commercial interests.

Areas where we encourage Ofcom to strengthen the codes are as follows:

Leveraging Industry Expertise and Fraud Intelligence

Ofcom should place greater emphasis on intelligence, expertise and evidence derived from sectors that routinely investigate fraud and respond to consumer harm. Financial institutions, law enforcement agencies, cyber-intelligence providers and fraud prevention organisations possess operational insights into criminal methodologies, emerging threats, confirmed fraud outcomes and organised criminal activity that may not be visible to Online Services. Incorporating these sources into risk assessments, moderation decisions and effectiveness reviews would support a more evidence-led and outcome-focused framework.

Measuring Outcomes - While governance and risk management requirements are welcome, effectiveness should be assessed through measurable reductions in fraud and consumer harm rather than compliance activity alone. Transparency reporting should support consistent assessment of scam losses, fraudulent advertising volumes, repeat offending, detection and removal times, and the effectiveness of preventative interventions.

Broader Fraud Risks Categories - Enhanced controls for FCA-regulated financial promotions in the proposals are welcomed and important but should not be the sole focus. Significant harm also arises from retail impersonation scams, fraudulent e-commerce sites, cryptocurrency scams, and speculative investment schemes. Controls should therefore apply across all high-risk advertising categories driven through risk-based monitoring and advertiser due diligence.

Continuous Improvement - Online Services should maintain structured feedback loops to ensure controls evolve alongside criminal methodologies. Repeated reports confirmed fraud incidents, and emerging fraud typologies should trigger reviews of policies, detection tools, and enforcement approaches.

Ad Libraries - Ad libraries have significant potential as operational fraud prevention tools. Ofcom should establish minimum standards covering advertiser attribution, verified advertiser information, advert content, URLs, enforcement outcomes, and appeal histories. Enhanced access for Ofcom and trusted organisations would improve intelligence sharing, oversight, and fraud disruption. Platforms should also actively utilise ad-library intelligence within their own moderation processes.

Clarification of Scope - Ofcom should clarify whether affiliate-driven placements, such as commission-based links and recommended-provider panels, fall within the

paid-for advertising regime. Greater clarity is also needed on how advertiser claims of third-party approval will be validated to prevent misuse of legitimate firms' credentials.

Collectively, these changes would move the framework from a largely reactive model to a preventative, intelligence-led, and outcome-focused approach that better protects consumers and disrupts fraud at scale

1. Context

Online Advertising Ecosystem

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

UK Finance believes Ofcom should explicitly recognise the value of payment-sector intelligence when identifying indicators of fraudulent advertising**.** Financial institutions hold unique datasets through scam investigations, APP fraud case reviews, chargeback activity, impersonation reporting and wider economic crime operations, UK Finance members frequently identify fraudulent advertising activity that is not visible through platform-based monitoring alone. In many instances, harm is first identified downstream, after a consumer has interacted with an advert, left the platform environment and suffered financial loss. This experience demonstrates the importance of incorporating external intelligence sources alongside platform-generated indicators.

More specifically chargeback data, FS industry scheme intelligence, and vendor data associated with fraudulent advertising activity may provide valuable indicators of:

- Compromised advertising accounts and account takeover activity.
- The use of stolen payment credentials to purchase advertisements.
- Organised criminal groups using online advertising to facilitate fraud, scams, and other forms of criminality.
- First-party fraud and abuse of advertising Online Services.
- Repeat offending advertisers and associated criminal infrastructure.

While these data sources are not, in isolation, definitive indicators of fraud, they can provide valuable intelligence when combined with other signals, such as account behaviour, advertiser verification data, moderation outcomes, fraud reports, and account takeover indicators. Our sector draws on a wide range of intelligence sources to support informed decision-making and the effective mitigation of evolving threats.

We therefore encourage Ofcom to recognise confirmed fraud intelligence and relevant payment-sector data as examples of information that providers may consider as part of their fraud risk and indicator assessments. This would support a more intelligence-led approach to fraud prevention and help Online Services identify high-risk advertisers and campaigns earlier in their lifecycle.

More broadly, UK Finance believes Online Services should be encouraged to develop mechanisms to receive and utilise external fraud intelligence where they consider it valuable to their fraud prevention efforts. This could include trends

derived from chargebacks, industry schemes, scam reports, vendor intelligence, and confirmed fraud outcomes, helping to strengthen not only the risk assessments, but also the moderation decisions, and proactive detection capabilities to mitigate consumer harm.

Online Services should be required to make appropriate use of relevant external intelligence as part of their fraud risk management and mitigation arrangements. It should be their responsibility to develop the governance, processes, and technical infrastructure necessary to utilise such intelligence effectively. Any sharing of intelligence should be proportionate, purpose-specific, and compliant with applicable legal, regulatory, and data protection requirements. Importantly, this should not result in additional obligations being placed on financial services firms.

Importantly, the availability or absence of financial sector intelligence should not diminish the responsibility of Online Services to maintain effective fraud prevention controls. Online Services should remain accountable for identifying, preventing, and disrupting fraudulent advertising through their own systems and processes. External intelligence should be viewed as a complementary enhancement to Online Services control framework, rather than a prerequisite for effective fraud mitigation.

Causes and Impacts of Fraudulent Advertising

Do you have any comments on Ofcom's assessment of the causes and impacts of fraudulent advertising?

We believe Ofcom's assessment understates the breadth and diversity of fraud and scam harms facilitated through online advertising. While considerable attention is rightly given to FCA-regulated financial promotions, consumers are increasingly targeted through a wider range of fraudulent investment and wealth-building schemes that fall outside the regulatory perimeter.

These products are frequently marketed using similar techniques to regulated investment scams, including exaggerated returns, false endorsements, urgency tactics and impersonation of legitimate organisations.

As a result, focusing controls predominantly on FCA-authorised financial promotions risks overlooking a substantial segment of fraud activity that consumers may reasonably perceive as investment opportunities. We therefore encourage Ofcom to adopt a broader, harm-based risk taxonomy covering regulated financial promotions, unregulated investment-style products, fake retail, impersonation, crypto and digital assets, payment diversion and card-harvesting journeys. Controls should be triggered by harm characteristics rather than regulatory classification alone which includes examples such as Card Fraud, Fake Storefronts and Credential Harvesting.

Ofcom should also explicitly recognise employment scams and fraudulent job advertisements as a significant source of money mule recruitment. Given the important role these adverts play in facilitating wider fraud and money laundering activity, money mule recruitment through fraudulent advertising should be identified as a core harm within the framework.

Profiting UK Finance members have repeatedly observed criminal groups using online advertising and promoted content to recruit money mules[2], facilitate account opening abuse and support wider organised criminal activity. While consumer financial loss is often the most visible outcome, fraudulent advertising frequently forms part of broader criminal ecosystems that enable fraud, money laundering and the movement of criminal proceeds.

Greater emphasis should also be placed on fraud enabled through data harvesting, rather than focusing solely on immediate financial loss. Fraudulent advertisements are frequently used to obtain personal, payment, and account information that can subsequently be exploited to facilitate other fraud types, including digital wallet fraud and account compromise. In addition, fraudsters often leverage compromised victims and hijacked accounts to target further individuals through trusted relationships and social networks, amplifying consumer harm beyond the initial interaction with the advertisement.

Approach to codes

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

As stated previously, we believe Ofcom has underestimated the scale and breadth of harm arising from fraudulent advertising. While the assessment focuses on several established fraud typologies, it does not fully reflect the wider range of consumer, economic and societal harms that can result from fraudulent advertisements. The harms arising from fraudulent advertising extend beyond direct financial loss and include:

Financial and Personal Harms

- Direct theft of consumer funds through fake investment opportunities, banking scams, payment fraud and cryptocurrency schemes.
- Identity theft through phishing advertisements designed to harvest credentials, personal information and payment card details.

[2] Lived experiences of money muling - GOV.UK

- Consumer losses arising from the purchase of counterfeit, defective or non-existent goods and services.

Market and Economic Harms

- Reputational damage to legitimate businesses whose brands, products or services are impersonated by fraudsters.
- Increased costs for businesses and consumers associated with fraud prevention, remediation and customer support.

Societal and Trust Harms

- Erosion of consumer trust in online advertising, digital Online Services, news sources and online commerce.
- Reduced confidence in legitimate digital services and innovation due to concerns regarding fraud and impersonation.
- Wider economic crime impacts where proceeds of fraud are used to support organised criminal activity.

UK Finance believes the Codes should establish a clear framework for allocating responsibilities across the advertising ecosystem. Responsibilities should be clearly defined between (i) Online Services, including advertiser onboarding, preventative controls, monitoring, moderation, and takedown/remediation activities; (ii) advertisers and intermediaries, including obligations relating to authenticity, compliance, and cooperation with Online Services controls; and (iii) financial institution engagement, including proportionate cooperation and intelligence sharing where lawful, alongside their existing regulatory obligations. This should not, however, result in the imposition of additional obligations on the financial services sector.

Clear delineation of responsibilities would strengthen accountability, reduce ambiguity, and help ensure that risks are managed by the parties best positioned to prevent and mitigate them. This would also guard against responsibility for Online Services -originated risks being transferred to other sectors and avoid an outcome where diffuse accountability undermines effective fraud prevention.

In addition, Online Services generate advertising revenue from activity that may subsequently be identified as fraudulent, creating a potential misalignment between short-term commercial incentives and investment in preventative controls. Ofcom should consider whether existing commercial incentives are sufficient to support sustained investment in preventative controls.

Consider whether:

- benefiting from such advertising could amount to receipt of criminal property; and
- offences under sections 327-329 of the Proceeds of Crime Act 2002 might become relevant where an Online Services knowingly benefits from criminal activity.

This introduces a wider policy question about whether regulatory intervention should focus not only on consumer protection but also on the financial incentives of Online Services.

There is also a legal question regarding causal links between:

- the fraudulent advert;
- the subsequent contact with the fraudster; and
- the eventual financial loss.

Ofcom should consider how revenue associated with advertising subsequently confirmed as fraudulent is treated when assessing the proportionality of preventative controls.

Combined impact assessment

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.

UK Finance supports proportional implementation, but all providers should meet a common baseline of fraud-prevention outcomes. The structure reflects good fraud prevention principles by seeking to prevent fraud at source, improve detection capabilities and ensure timely remediation when harmful content is identified. The combination of governance, account verification, moderation, reporting and AI controls creates a stronger framework than any single intervention would achieve in isolation.

The proportionality framework gives platforms considerable discretion over the extent of measures they implement, rather than requiring specific safeguards or sustained, outcome-focused investment. In practice, platforms may be able to demonstrate compliance through policies, governance arrangements and reactive moderation, without deploying the most effective system-wide controls capable of materially reducing harm. However, there remain several important gaps from a fraud and scam prevention perspective.

1. Insufficient Focus on Outcomes

While Ofcom estimates significant economic benefits from the package, the proposed controls are largely measured through implementation rather than effectiveness.

There is limited emphasis on performance indicators such as:

- Reduction in scam losses.
- Reduction in consumer harm.
- Reduction in fraudulent impressions served.
- Removal times.
- Repeat offender rates.

Without outcome-based measures there is a risk that compliance becomes focused on demonstrating activity rather than reducing fraud.

2. Limited Use of Confirmed Fraud Intelligence

The framework relies heavily on Online Services generated indicators. However, some of the strongest evidence of fraud sits outside Online Services, including:

- APP fraud reports & Scam victim reports. Our members routinely utilise confirmed fraud outcomes, reimbursement cases, mule account intelligence and scam reporting data to assess the effectiveness of fraud controls. Lessons learned from confirmed fraud events are a cornerstone of modern fraud risk management. It is therefore notable that equivalent expectations are not reflected more strongly within the proposed framework for Online Services.
- Banking intelligence.
- Chargeback, industry scheme and vendor intelligence and data.
- Law enforcement intelligence.

For example, Card Scheme chargeback reports, industry fraud data and some supplier data and intelligence relating to advertising spend can provide indicators of:

- Account takeover.
- Stolen payment card usage.
- First-party fraud.
- Organised criminal activity.
- Fraudulent advertisers.

The proposals do not sufficiently encourage the use of these external intelligence sources within fraud indicator assessments.

3. Weak Feedback Loops

The framework does not adequately address situations where:

- Advertisements are repeatedly reported.
- Reports are rejected due to policy limitations.
- Consumer harm subsequently occurs.

These scenarios should trigger policy reviews and reassessment of moderation approaches. Without formal feedback loops, Online Services risk repeatedly applying policies that fail to identify emerging threats. This should be reviewed either via audit and or the transparency reports showing effectiveness of these mechanisms.

4. Limited Supply Chain Accountability

While the proposals recognise advertising intermediaries, there is insufficient focus on measuring intermediary performance. Providers should maintain contractual and operational controls over intermediaries, including fraud-prevention standards, audit rights, verification requirements, response-time expectations, reporting by intermediary and consequences for repeated control failures.

Additional missing considerations include:

- Fraud rates by intermediary.
- Where credible indicators suggest an immediate risk of serious consumer harm, providers should be able to apply proportionate interim restrictions, pending investigation.
- Repeat control failures.
- Response times.
- Audit outcomes.

Criminals frequently exploit weaknesses in complex advertising supply chains, making intermediary oversight critical.

5. No Clear Definition of "Swift"

The layered approach depends heavily on rapid remediation once fraudulent advertising is identified. For confirmed fraudulent adverts or trusted-flagger reports, Ofcom should require immediate evidence preservation, rapid triage, defined review timelines and time bound restriction/removal. High-risk categories such as investment scams, impersonation and account takeover should attract shorter escalation timelines. However, Ofcom does not currently define:

- Expected review times.
- Removal targets.
- Escalation timelines.
- Trusted flagger service levels.

Without clearer expectations, performance could vary significantly between providers, and this would lead to inconsistent outcomes and consumer safety

expectations across Online Services. These expectations should be risk-based and focused on high-confidence fraud indicators and trusted-flagger reports, rather than applying identical performance standards across all providers and all forms of content.

6. Insufficient Focus on Repeat/Cross Sector Offending

The proposals discuss account bans but provide limited detail regarding:

- Linked account detection.
- Cross-Online Services enforcement.
- Repeat advertiser identification.
- Ban evasion.
- "Phoenixing" behaviour.

This is a significant fraud risk because organised criminal groups routinely create replacement accounts after enforcement action.

7. Narrow View of Harm

The benefits assessment recognises financial loss and wider societal harms but may underestimate the range of fraud-related harms arising from advertising.

These include:

- Identity theft and recovery.
- Account compromise and recovery.
- Retail impersonation scams, trust erosion.
- Purchase of counterfeit or non-existent goods.

The framework would benefit from a broader, harm-based assessment of fraud risks.

8. Ad Libraries Underutilised

Ad libraries are positioned largely as transparency tools. However, members believe they should become operational fraud prevention tools used by Online Services themselves for:

- Detection, including linked campaigns and related adverts.
- Intelligence sharing.
- Campaign disruption.
- Intermediary identification
- Repeat offender identification.
- Consumer protection.

Overall, the proposal provides a strong foundation and correctly adopts a prevention-detection-remediation model. However, from a fraud and scams perspective, the framework remains strongest on **process and governance** and weaker on

measurement, intelligence integration, feedback loops and demonstrable outcomes.

The most important enhancements would be:

1. Outcome-based performance measures.
2. Incorporation of confirmed fraud and payment-sector intelligence.
3. Stronger feedback loops where reports lead to confirmed harm.
4. Greater accountability across advertising supply chains.
5. Defined remediation and takedown expectations.
6. More operational use of ad libraries.
7. Broader recognition of scam harms beyond regulated financial promotions.

Lastly, revenue attributable to advertising that is found to be fraudulent should not be treated as a legitimate economic benefit when assessing the proportionality of preventative measures. These changes would help move the framework from a compliance-focused model to one that demonstrably reduces fraud and consumer harm.

2. Risk, Governance, and Control

UK Finance members support Ofcom's proportionality-based approach, recognising that obligations must be calibrated according to Online Services size, functionality, user reach and risk profile. However, we believe the effectiveness of this approach depends heavily on the underlying assessment of fraud harms and risks. Ofcom's assessment should fully reflect the breadth of fraud typologies facilitated through online advertising and the significant harm these can cause.

Fraudulent advertising extends beyond traditional financial promotions and includes:

- Investment scams involving unregulated assets.
- Retail impersonation scams.
- Cryptocurrency and digital asset fraud.
- Medical and Insurance advertising
- Fake customer support advertising.
- Payment diversion scams.
- Fraudulent e-commerce and marketplace activity.

We encourage Ofcom to expand its assessment of fraud indicators and risk characteristics to reflect how criminals adapt campaigns across different demographics, products, geographies and advertising formats. Attention should be given to evolving tactics such as rotating advertisements, cloned campaigns, synthetic identities and AI-generated content designed to evade moderation.

While we recognise Ofcom must balance safety duties against wider considerations such as privacy and freedom of expression, we believe the codes should fully account for the breadth of consumer, economic and societal harms caused by fraudulent advertising when determining the proportionality of controls. Also, the proposed accountable individual does not appear to be subject to an equivalent Senior Managers Regime or comparable personal accountability framework. We therefore encourage Ofcom to consider whether the proposed governance arrangements create sufficient incentives and accountability to drive effective fraud prevention outcomes, or whether additional measures may be required to ensure meaningful ownership of fraud risk and mitigation activities at a senior level.

Advertising Intermediaries

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

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.

UK Finance members support the flexibility provided by the "all reasonable endeavours" approach, recognising the complexity of advertising supply chains and varying levels of provider control. However, we believe Ofcom should enhance this principle so that Online Services are required rather than encouraged to act and have clearer expectations regarding the outcomes providers should seek to achieve. Process-based evidence alone may not sufficiently demonstrate that reasonable endeavours have delivered equivalent consumer protection outcomes.

We therefore encourage Ofcom to establish outcome-focused measures and performance indicators that help assess whether alternative arrangements are effectively reducing fraudulent advertising and associated consumer harm. Such measures could include reductions in fraudulent advertisements served, improvements in takedown performance, reductions in repeat offending advertisers, and the effectiveness of controls implemented through advertising intermediaries.

In short, whilst Ofcom should not prescribe a single universal performance target across all providers, we believe it should establish minimum service expectations for high-confidence fraud referrals and define common outcome measures that enable performance to be assessed consistently. This would allow implementation to remain proportionate while ensuring that providers are accountable for achieving effective consumer protection outcomes. Outsourcing can also lead to avoidance of responsibility.

UK Finance notes a recurring concern among members regarding assertions that fraudulent advertising is inherently difficult to detect. While fraudsters continuously adapt their tactics, many Online Services already possess significant visibility of advertiser behaviour, account activity, payment information, content patterns, engagement signals, and network-level indicators that could support the identification of fraudulent advertisements and associated threat actors.

We therefore encourage Ofcom to place greater emphasis on the capabilities and responsibilities of Online Services to utilise the information, technology, and intelligence already available to them to identify and disrupt suspicious advertisers, fraudulent campaigns, and organised criminal activity. While no single control will detect all fraud, Online Services should be expected to demonstrate that they are making effective use of available tools, data, and detection capabilities to proactively

mitigate risks rather than relying predominantly on user reports or post-harm interventions.

The Codes should also recognise that effective fraud prevention is an outcomes-based challenge. Providers should be able to evidence how their systems and controls identify, prevent, and disrupt fraudulent advertising, and how those controls are contributing to measurable reductions in consumer harm.

- Online Services should be able to deploy AI and automated controls more aggressively. Examples include:
    - detecting clearly implausible AI-generated advertisements;
    - detecting use of well-known logos and brands;
    - identifying use of celebrities and public figures;
    - validating whether advertisers have authority to use intellectual property or endorsements.

The underlying view is that given providers' advanced use of automated systems in advertising delivery and optimisation, Ofcom should expect proportionate investment in automated capabilities designed to detect suspicious advertising and associated behaviour.

Supply Chain Accountability Gap

The proposal does not sufficiently address accountability where advertising intermediaries are involved in the delivery, placement, verification, or onboarding of advertisements. UK Finance believes that fraud risk cannot be outsourced. Providers should remain accountable for fraud prevention outcomes regardless of whether services are delivered directly or through intermediaries, and consumer protection outcomes should be consistent across the advertising supply chain.

Intermediaries must not become weaker points of control. Where providers rely on third parties for activities such as advertiser onboarding, identity verification, or due diligence, they should be expected to maintain appropriate oversight and assurance arrangements. This should be like regulated third-party oversight models in financial services, financial institutions have extensive experience managing critical third-party and outsourcing arrangements, including circumstances where customer-facing activities are undertaken by external providers. Industry experience demonstrates that accountability cannot be delegated and that effective oversight requires measurable outcomes, ongoing assurance, performance monitoring and escalation where control weaknesses are identified.

To support this, Ofcom should clarify whether providers are expected to monitor intermediary performance through measurable indicators such as:

- Intermediary response times.
- Fraud detection rates.
- Verification success rates.
- Repeat control failures.
- Volumes of fraudulent advertisements associated with intermediaries.

Providers should also be expected to demonstrate that their arrangements with intermediaries are delivering effective consumer protection outcomes through metrics such as:

- Reductions in fraudulent advertisements served.
- Reductions in repeat offending advertisers.
- Reductions in scam-related consumer harm.
- Reductions in advertisements originating from non-compliant intermediaries.
- Time taken to remove confirmed fraudulent advertisements.
- Percentage of trusted flagger reports actioned.
- Number of repeat incidents linked to the same intermediary.

These measures would help ensure that the use of intermediaries does not dilute accountability and would provide evidence that alternative delivery models are achieving safety outcomes comparable to those expected where controls are operated directly by the provider.

Record-Keeping

UK Finance members support Ofcom's proposed record-keeping requirements and recognise the importance of documenting instances where providers are unable to implement specific measures within the Codes. Maintaining records of decisions, governance processes and alternative controls can support accountability and provide Ofcom with greater visibility of how providers are managing fraud risks.

However, we believe the proposal is currently focused primarily on governance and procedural compliance rather than the effectiveness of controls in preventing fraud and reducing consumer harm.

The framework should also distinguish between standard record-keeping and event-triggered evidence preservation. Where an advert, advertiser, landing page, domain, payment route or linked account is associated with confirmed fraud intelligence, providers should be required to preserve relevant artefacts immediately so that subsequent investigation and disruption activity are not undermined by data loss.

Ofcom should require providers to assess whether alternative measures achieve equivalent fraud-prevention outcomes. As drafted, providers could demonstrate compliance through record-keeping and governance processes without evidencing whether controls have reduced fraudulent advertising, repeat offending or consumer

harm. The requirements should therefore incorporate outcome-based measures alongside process-based records.

Providers should be expected to maintain records relating to:

- Confirmed instances of fraud linked to advertising activity.
- Fraud reports received from trusted parties and whether action was taken.
- Cases where advertisements were reported but not removed and subsequently resulted in confirmed consumer harm.
- Repeat offending advertisers and attempts to evade enforcement action.
- The effectiveness of alternative controls implemented where a proposed measure could not be adopted.

This would provide a stronger basis for assessing whether controls are delivering outcomes comparable to those envisaged by the Codes.

We also believe the proposal places insufficient emphasis on the role of external intelligence. Financial institutions, fraud prevention bodies, law enforcement and trusted reporting organisations often have visibility of fraud activity long before it becomes apparent through Online Services monitoring. Providers should therefore maintain records of intelligence received from external sources, how that intelligence was assessed, and the actions taken as a result. This would help ensure that risk assessments and control decisions are informed by evidence of actual consumer harm rather than exclusively by Online Services -generated data.

In addition, there is an opportunity to strengthen the treatment of advertising supply-chain risks. While the proposal refers to engagement with advertising intermediaries, providers should also be expected to record information relating to intermediary performance, verification failures, enforcement actions and identified fraud risks. This would support more effective oversight of the wider advertising ecosystem and encourage accountability throughout the supply chain.

UK Finance also believes providers should retain information relating to repeat offending and ban evasion. Our members report that fraudsters seek to re-enter Online Services using new accounts, altered identities or associated entities following enforcement action. Recording attempts to circumvent controls, together with any linked accounts or associated infrastructure identified, would help providers and Ofcom assess whether preventative controls are operating effectively.

We also note that some fraud typologies, particularly investment scams and other long-duration frauds, may not be identified until a considerable period after the advertisement was first displayed. Ofcom should consider whether a retention period of at least five years is more appropriate for fraud-related records, particularly where consumer harm may not be identified until a considerable period after exposure. A longer retention period would support fraud investigation, trend analysis, repeat-offender identification and wider disruption activity.

Finally, we believe there would be value in introducing greater standardisation to record-keeping expectations. Without a common framework, providers may capture information in different ways, making comparisons difficult and limiting Ofcom's ability to assess effectiveness across services. Establishing a set of core records and outcome metrics would improve consistency, strengthen transparency reporting and facilitate more meaningful regulatory oversight.

Overall, UK Finance members support the principle of the proposed record-keeping requirements. However, we recommend that the framework be strengthened to capture consumer harm outcomes, confirmed fraud intelligence, repeat offending behaviour, supply-chain risks and evidence of control effectiveness. This would better align the requirements with the overarching objective of reducing fraudulent advertising and protecting consumers from harm.

Fraud Indicator Assessment

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

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?

UK Finance members support Ofcom's proposal requiring providers to undertake fraud indicator assessments and identify characteristics associated with fraudulent advertising. We agree that providers should assess indicators across advertisement content, advertiser accounts, account behaviour, targeted users and Online Services functionalities.

Ofcom should require fraud indicator assessments to connect advert content, advertiser identity, account behaviour, landing-page infrastructure, payment journey indicators and confirmed harm data. Treating the advert in isolation risks missing how scam journeys operate in practice, particularly where consumers are moved off-Online Services before payment or reporting occurs

We believe the examples and expectations should also be expanded to better reflect the sophistication and evolving nature of fraud threats observed across the financial services sector.

In particular, providers should be expected to consider indicators including:

Content of the Advertisement

- Impersonation of regulated firms, trusted brands, public bodies or well-known individuals.

- Use of manipulated media, deepfakes, synthetic endorsements or AI-generated content.
- Repeated use of substantially similar creative content across multiple advertisers or campaigns. This is frequently seen by our members.

Advertising Accounts

- Frequent changes to account ownership, business details or advertiser identity.
- Links to previously suspended or banned advertisers.
- Use of unverifiable business information or indicators that account verification has been circumvented.
- Patterns consistent with account takeover or misuse of legitimate advertiser accounts.

Account Behaviour

- Rapid creation and removal of advertisements.
- Frequent editing of advertisements following moderation reviews.
- Rotation of substantially similar advertisements to evade detection.
- Unusually high volumes of advertising activity within a short period.
- Behaviour indicative of coordinated campaigns operating across multiple accounts.
- Attempts to reactivate previously suspended advertising campaigns outside normal business hours.

Targeted Users

- Disproportionate targeting of vulnerable consumers.
- Targeting based on age, financial circumstances or characteristics commonly associated with scam victimisation.
- Repeated targeting of consumers following interactions with financial, investment or crypto-related content.
- Geographic targeting patterns associated with known fraud campaigns.

Service Functionalities

- Exploitation of recommendation systems to increase visibility of fraudulent content.
- Functionality that enables rapid recreation of previously removed advertisements or advertiser accounts.
- Online Services features that allow fraudsters to obscure advertiser identity or avoid moderation processes.

Many of the indicators outlined above are not theoretical risks. UK Finance members regularly encounter these behaviours during investigations into impersonation scams, investment fraud, account compromise and organised criminal activity. Repeated content reuse, rapid campaign rotation, links between previously removed

accounts and coordinated activity across multiple identities are established indicators that are already utilised by fraud teams across the financial sector.

Intelligence-Led Approach

We also recommend that Ofcom explicitly encourage providers to incorporate relevant external intelligence into their fraud risk assessments. Online Services should have mechanisms capable of receiving, assessing, and acting upon relevant external intelligence, recognising that fraud indicators should not be determined solely by information available within an Online Services 's own environment.

Relevant sources of intelligence may include:

- Confirmed fraud and scam intelligence.
- Industry information-sharing arrangements, which Ofcom should actively encourage.
- Law enforcement intelligence.
- Cyber threat intelligence providers.
- Trusted flagger referrals.
- Insights derived from previous reports of fraudulent advertising that subsequently resulted in confirmed consumer harm.

Ensuring that Online Services can effectively utilise relevant external intelligence will strengthen their ability to identify emerging threats, detect fraudulent activity more quickly, and implement preventative measures before significant consumer harm occurs.

Dynamic Review of Indicators

While UK Finance members support the proposed review cycle, fraud indicator assessments should be treated as dynamic and continuously updated rather than annual compliance exercises. Providers should be expected to reassess indicators whenever:

- New fraud typologies emerge.
- Significant scam losses are identified.
- Repeat reports expose weaknesses in moderation policies.
- Intelligence from trusted partners identifies evolving criminal tactics.

This would help ensure that fraud assessments remain relevant and effective in a rapidly evolving threat landscape and support Ofcom's objective of reducing consumer harm from fraudulent advertising. Several indicators identified by Ofcom seem inherently measurable, including:

    - advertiser account creation patterns;
    - abnormal payment activity;

- use of known brands and logos;
- use of celebrity endorsements;
- linked account networks;
- unusual targeting behaviour; and
- suspicious account changes.

Online Services must use those same indicators proactively to identify and remove fraudulent advertising.

Governance and Accountability

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

The principal weakness of the proposals is that they focus primarily on demonstrating that Online Services have processes and controls in place, rather than evidencing whether those controls are effectively preventing fraud and reducing consumer harm. To strengthen the regime, UK Finance advocates four key enhancements: a greater emphasis on outcome-based measurement, transparency reporting, and the publication of performance data; increased use of confirmed fraud intelligence and relevant payment-sector data; stronger feedback mechanisms that incorporate evidence of actual consumer harm and fraud outcomes; and clearer accountability for repeat offenders, intermediaries, and the effectiveness of moderation activities. Collectively, these measures would help shift the framework from a process-driven compliance model towards one that is more transparent, accountable, and focused on delivering measurable reductions in fraud.

We believe the focus on outcome-based measurement should be significantly strengthened through mandatory transparency and publication requirements. Similar to reporting obligations within the APP fraud regime, Online Services should be required not only to collect and submit performance data to Ofcom, but also to publish key metrics, outcomes, effectiveness assessments, and the results of any independent review. This information should be made available in a clear, accessible, and consumer-friendly format, ideally through providers' corporate websites and, where appropriate, directly within their Online Services or apps.

Greater transparency would enable consumers to make informed decisions about the Online Services they choose to engage with and the businesses advertising on them. It would also create stronger incentives for Online Services providers to improve performance and accountability, while enabling financial institutions, researchers, and wider civil society to scrutinise trends, identify emerging risks, and contribute to the intelligence-sharing ecosystem.

While the proposed measures represent a positive step forward, many of the controls continue to rely heavily on provider self-assessment and self-reporting. The financial sector's experience with operational resilience, fraud prevention and financial crime regulation demonstrates that self-attestation alone is rarely sufficient to evidence effectiveness. Independent assurance, testing and external scrutiny have proven valuable in identifying weaknesses that may not be apparent through internal governance processes.

To strengthen confidence in the regime and ensure that controls are delivering measurable reductions in fraud, we recommend:

- Independent audits of Online Services controls and performance.
- Standardised metrics and transparency reporting benchmarks. Standardised reporting should distinguish prevention from post-publication detection and removal. Metrics should include the proportion of fraudulent adverts blocked before publication, user exposure or impressions, time to detection and removal, recurrence and repeat-offender rates, and downstream confirmed harm. Ofcom should define common denominators and reporting methodologies so that performance is comparable across services and cannot be overstated through activity measures alone.
- Cross-sector performance comparisons.
- Regular Ofcom-led effectiveness reviews.

Without independent validation and publicly available performance data, it will be difficult to determine whether controls are genuinely reducing fraud and consumer harm. These enhancements would help move the regime beyond a process and compliance-focused approach towards a transparent, evidence-based, and genuinely intelligence-led fraud prevention framework.

For higher-risk providers, Ofcom should require periodic independent testing of fraudulent advertising controls. This should include sample testing of moderation decisions, trusted-flagger outcomes, repeat-offender controls, ad-library completeness and evidence-retention performance. Without independent validation, it may be difficult to assess whether controls are genuinely reducing fraud.

Ad Libraries Are Treated Primarily as Transparency Tools

The proposals recognise the value of ad libraries, but do not fully exploit their fraud prevention potential. Ad libraries should support:

- Fraud investigations.
- Campaign disruption.
- Repeat offender detection.
- Cross-Online Services intelligence sharing.
- Proactive fraud monitoring.

Online Services should be expected to actively use ad libraries themselves rather than solely relying on external stakeholders to identify harmful content.

Where reporting, audit or independent testing identifies persistent poor outcomes, Ofcom should require proportionate escalation, including time-bound remediation plans, enhanced reporting, targeted independent assurance and, where failures continue, enforcement action. This would create a clear link between evidence of poor performance and supervisory consequences.

Weak Feedback Loops

The framework does not sufficiently address situations where:

- Fraudulent adverts are reported.
- Reports are rejected.
- Consumer harm subsequently occurs.

These circumstances should trigger:

- Policy reviews.
- Detection model reviews.
- Moderator training improvements.
- Updates to fraud indicators.

Without structured feedback loops, known weaknesses may persist. The feedback loop effectiveness should be assessed within the audit processes and or the transparency reporting.

Leveraging Intelligence Beyond Consumer Reporting

UK Finance members support the introduction of advertising complaints mechanisms and recognise that user reports can provide valuable intelligence regarding fraudulent advertising. However, we are concerned that the proposed framework places significant reliance on consumer reporting as a means of identifying fraud.

In practice, many victims do not report fraudulent advertisements, and consumers are increasingly faced with sophisticated scams that closely mimic legitimate content. The growing use of impersonation techniques, synthetic media, and AI-enabled advertising means that consumers often have little realistic opportunity to distinguish fraudulent advertisements from genuine ones before harm occurs. As a result, fraudulent advertising is frequently identified only after financial losses have been incurred or other forms of harm have materialised. While consumer awareness remains an important component of fraud prevention, it should not be viewed as the primary mechanism for mitigating risks that originate within advertising ecosystems.

Given their visibility of advertiser activity, user engagement, payment flows, and behavioural signals. Online Services are uniquely positioned to identify and disrupt fraudulent advertising before consumers are harmed. Greater emphasis should therefore be placed on the responsibility of Online Services to implement effective preventative controls and to take reasonable steps to protect users, particularly those who may be vulnerable to fraud. Online Services should consider what additional safeguards can be deployed where users have interacted with, engaged with, or been exposed to suspected fraudulent advertising. These could include targeted warnings, tailored interventions, enhanced monitoring of repeat exposure, and other measures designed to reduce the risk of further victimisation.

While it is unrealistic to expect that all fraudulent advertisements can be prevented, Online Services should be expected to demonstrate that they are delivering effective outcomes for consumers and meeting an appropriate standard of care. This includes maintaining robust systems and controls to identify, assess, and mitigate fraud risks, as well as providing appropriate support and protections where harm occurs.

We therefore encourage Ofcom to place greater emphasis on proactive and intelligence-led detection measures, including automated monitoring, behavioural analysis, advertiser risk profiling, fraud indicator assessments, and the use of relevant internal and external intelligence sources. Consumer complaints and user reports remain valuable sources of information, but they should be regarded as one input among many rather than the primary means of identifying fraudulent advertising. An effective fraud prevention framework should focus on detecting and disrupting malicious activity before consumers are required to identify and report it themselves.

Greater Use of External Fraud Intelligence

We also believe the proposals do not sufficiently recognise the value of intelligence held outside of Online Services.

Ofcom should therefore encourage providers to incorporate external intelligence sources into their fraud prevention, moderation and risk assessment processes. A more intelligence-led approach would improve the identification of emerging threats, accelerate remediation activity and strengthen the overall effectiveness of Online Services controls.

Incorporating Confirmed Fraud Data

More specifically, we believe there is insufficient emphasis on the use of confirmed fraud data to inform Online Services decision-making.

The proposals currently focus heavily on Online Services generated indicators and moderation signals. While these are important, they should be supplemented by intelligence derived from actual instances of consumer harm. Examples include:

- Authorised Push Payment (APP) fraud data.
- Scam victim reports.
- Reimbursement and remediation cases.
- Mule account intelligence.
- Chargeback, industry scheme and Vendor and disputed transaction data.

Of relevance is chargeback, industry scheme and vendor intelligence associated with advertising activity. While this data sources alone are not a definitive indicator of fraud, they may provide valuable signals relating to account takeover, the use of stolen payment credentials, organised criminal activity and fraudulent advertiser behaviour.

When combined with Online Services data, advertiser verification information and behavioural indicators, this intelligence has the potential to significantly enhance fraud detection capabilities and improve advertiser risk assessments. UK Finance therefore encourages Ofcom to recognise confirmed fraud intelligence as an important source of evidence that should inform fraud indicator assessments, moderation processes and the ongoing development of Online service controls.

Online Services should also be required to establish clear and transparent processes for notifying affected parties when advertising content is restricted, removed, or blocked. This should include timely notification, clear reasons for the action taken, and an effective escalation and appeals process. Importantly, these arrangements should recognise that advertisers are not always the only stakeholders affected by such decisions. Publishers, affiliates, and other commercial partners may also incur costs or experience adverse impacts where placements are withdrawn. Without appropriate procedural safeguards, legitimate parties may be left bearing financial consequences without sufficient notice or an opportunity to address or rectify identified issues. Clear and proportionate processes would support fairness, improve compliance, and reduce the risk of unintended harm to legitimate businesses.

Testing Advertisement Generation Tools

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

UK Finance members support Ofcom's proposal to require testing of advertisement generation tools and welcomes the recognition that AI systems can be exploited to facilitate fraudulent advertising. However, the framework remains heavily focused on governance, testing and provider-controlled tools. We believe it should place greater emphasis on fraud outcomes, external intelligence sources, organised criminal abuse, account takeover risks and the detection of AI-generated fraud regardless of where content is created. Providers should be encouraged to incorporate confirmed fraud intelligence, including scam reports and payment-sector data, into their testing and risk assessment processes. This would help ensure that safeguards evolve in response to real-world criminal activity and consumer harm, rather than solely Online Services -generated indicators.

3. Ensuring Account Integrity

Account Checks and Actions

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:

a) verification that advertising account holders work for, or on behalf of, the individual or organisation they are advertising;

b) checks and actions to prevent banned advertising account holders returning; and

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.

d) repeat checks where there are relevant changes identified on an account.

Repeat checks should be triggered by material changes to advertiser identity, account ownership, creative content, destination URLs or redirect chains, payment methods, targeting parameters or other indicators of elevated risk. Where the change is material, re-screening should occur before further delivery where proportionate to the risk.

• 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.

Gaps and Areas for Enhancement from a Fraud and Scams Perspective

UK Finance supports Ofcom's proposed account checks and actions. The framework should require effective verification of authority to advertise, controls preventing banned advertisers from returning, enhanced checks for materially higher-risk accounts, and repeat checks where relevant account or campaign information. The proposal appropriately recognises the growing role that AI-enabled tools may play in the creation and scaling of fraudulent content and seeks to establish governance, testing and accountability mechanisms to mitigate these risks.

These checks should operate as an ongoing, risk-based control rather than a one-off onboarding exercise and should connect advertiser identity, account behaviour, payment arrangements, campaign content and linked infrastructure.

Scope of Advertisement Generation Tools

The proposal focuses primarily on advertisement generation tools made available by the Online Services itself. While this is an important starting point, fraudsters increasingly utilise a wide range of third-party and external AI tools to create fraudulent advertising content before uploading it to Online Services.

As a result, the risk to consumers is not limited to Online Services -owned tools. We therefore encourage Ofcom to consider whether providers should also be expected to develop controls capable of identifying and detecting AI-generated fraudulent content irrespective of where that content was created.

Greater Use of Confirmed Fraud Intelligence

We recommend that Ofcom encourage providers to incorporate external fraud intelligence into testing programmes, fraud indicator assessments and risk management processes.

Organised Criminal Abuse and Campaign-Level Risks

The proposal largely focuses on whether individual advertisements can be generated through misuse of AI tools. However, organised criminal groups typically operate at a campaign level, deploying multiple advertisements, identities, domains and accounts simultaneously. Providers should therefore be encouraged to assess how advertisement generation tools may facilitate:

- Large-scale scam campaigns.
- Coordinated impersonation activity.
- Automated generation of multiple fraudulent advertisements.
- Rapid regeneration of content following enforcement action.

This would create a more realistic assessment framework better aligned with the threat environment observed by industry.

Account Takeover and Fraudulent Advertiser Activity

The consultation does not appear to sufficiently consider the interaction between advertisement generation tools and compromised advertising accounts.

A legitimate advertiser account that has been taken over by a criminal actor could potentially be used to create and distribute fraudulent advertisements at scale, while benefiting from existing trust signals associated with the account.

We therefore recommend that testing scenarios include account takeover risks and the misuse of legitimate advertiser accounts for the AI tools features.

Feedback Loops and Continuous Improvement

The proposal requires providers to maintain logs and document vulnerabilities but places less emphasis on learning from instances where controls have failed. Where AI-generated advertisements subsequently result in confirmed fraud, providers should be expected to review:

- Whether vulnerabilities were previously identified.
- Whether safeguards were adequate.
- Whether testing methodologies require enhancement.
- Whether additional controls should be implemented.

This would support a more dynamic and continuously improving control environment.

Measurement of Effectiveness

Finally, while the proposal includes requirements for testing and governance, there is limited emphasis on measuring outcomes.

In addition to documenting testing activity, providers should be encouraged to assess:

- Reductions in AI-enabled fraudulent advertising.
- Detection rates for AI-generated scams.
- Fraud losses linked to AI-generated advertisements.
- Time taken to identify and remove AI-enabled fraudulent content.

Without outcome-based measures, there is a risk that compliance focuses on demonstrating testing activity rather than evidencing reductions in fraud and consumer harm.

Conclusion

UK Finance members support Ofcom's objectives and agree that advertisement generation tools present an increasing fraud risk. However, the framework would be strengthened by incorporating external fraud intelligence, expanding consideration of organised criminal activity and account takeover risks, introducing stronger feedback mechanisms, and placing greater emphasis on measurable fraud prevention outcomes. This would help ensure the controls remain effective against rapidly evolving scam and fraud threats.

Preventing Fraudulent Financial Services Advertising

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

UK Finance strongly supports Ofcom's proposal to introduce a financial services verification regime and welcomes the recognition that investment scams and fraudulent financial promotions continue to drive significant consumer harm. The requirement to verify FCA authorisation status and assess firms against the FCA Warning List represents a substantial improvement on existing voluntary arrangements.

Streamlined Verification for Authorised Firms

UK Finance recommends that Ofcom consider a proportionate "fast lane" approach for FCA-authorised firms. Once an Online Services has verified an advertiser's FCA authorisation and established core account controls, firms should not be required to repeatedly demonstrate their identity or regulatory status for each campaign or channel. This would reduce unnecessary friction for legitimate advertisers and allow Online Services to focus resources on higher-risk, unauthorised, or potentially fraudulent advertisers.

The fast lane should remove unnecessary repetitive verification, but should not replace ongoing monitoring, behavioural controls, or risk-triggered re-verification where indicators of account compromise, misuse, or elevated fraud risk are identified.

To avoid creating vulnerabilities, such an approach should be supported by ongoing monitoring and risk-based triggers designed to detect issues such as account compromise, misuse, or account takeover**.** Fraud and Scams perspective, there are several areas where the proposal could be strengthened.

Scope is Too Narrow and Risks Creating Regulatory Displacement

The proposal is primarily focused on financial services advertising and advertisements subject to the financial promotions regime. While this addresses an important segment of fraud, consumers are increasingly targeted through scams that fall outside the FCA regulatory perimeter.

Examples include:

- Whisky, wine and other alternative investment scams.
- Carbon credit schemes.
- Rare earth mineral investments.

- Property investment scams.
- Fake retail investment opportunities.
- Cryptocurrency promotions that may sit outside current authorisation requirements.
- Wealth generation and "get rich quick" schemes.

The industry has observed that criminals adapt their tactics to exploit gaps between regulatory frameworks. There is therefore a risk that stronger controls around regulated financial promotions simply displace fraudulent activity into adjacent categories that present similar levels of consumer harm.

We encourage Ofcom to consider a broader, harm-based approach that captures advertisements presenting significant investment or financial risk to consumers, irrespective of whether they are formally classified as financial promotions.

We recommend that Ofcom require Online Services to apply enhanced checks to investment-like and wealth-generation advertising where the product presents similar consumer harm to regulated financial promotions, even if it falls outside the FCA perimeter.

Verification Does Not Fully Address Account Takeover Risks

The proposal focuses on verifying that advertisers are authorised at the point of onboarding. However, fraud risks do not end once verification has been completed.

It has been reported that criminals increasingly compromise legitimate businesses and advertising accounts to exploit established trust and reputation. A legitimate FCA-authorised firm whose account has been compromised could still be used to distribute fraudulent advertising.

We therefore encourage Ofcom to place greater emphasis on:

- Ongoing and enhanced account monitoring.
- Behavioural analytics.
- Account takeover detection.
- Enhanced authentication controls.
- Re-verification following suspicious activity.

Lack of Cross-Online Services Intelligence Sharing

The proposals operate largely at an individual Online Services level. However, fraudsters often operate across multiple services simultaneously and may migrate activity following enforcement action.

We recommend that Ofcom consider how Online Services can support the sharing of intelligence relating to:

- Banned advertisers.
- Fraudulent domains.

- Known scam typologies.
- High-risk identities.
- Repeat offenders.

A more coordinated approach would reduce opportunities for criminals to move between services.

We encourage Ofcom to consider requiring reporting against outcomes such as:

- Reductions in scam losses.
- Volumes of financial scam advertisements removed.
- Number of prevented fraudulent advertisers.
- Repeat offending rates.
- Detection and removal times.

Without outcome measures, it may be difficult to assess whether the verification regime is delivering meaningful reductions in consumer harm.

Feedback Loops Could Be Stronger

The proposal includes annual reviews and policy updates but does not explicitly require learning from incidents where fraud has occurred.

Where:

- Advertisements pass verification and later result in consumer harm;
- Fraudulent advertisers evade detection;
- Trusted reports identify weaknesses in the framework; or
- New scam methodologies emerge,

providers should be expected to review and strengthen their controls accordingly. This would help ensure the verification framework evolves alongside the threat landscape.

Payment Route Traceability

Advertiser verification should extend beyond identity verification and include traceability of advertising payments. Providers should retain information linking advertisers to the payment methods used to purchase advertising inventory, associated payment accounts, payer details and any subsequent changes to payment arrangements. This information should form part of fraud investigations, repeat-offender detection and evidence-preservation requirements. Criminal actors frequently reuse payment infrastructure across multiple advertising accounts and campaigns. Maintaining these links enables more effective identification of organised criminal activity and supports enforcement against repeat offenders.

Countering Account Takeover

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

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

UK Finance members support Ofcom's proposal to require robust account security mechanisms for advertising accounts and agrees that account takeover is a significant enabler of fraudulent advertising. Strong authentication, account recovery processes, periodic security reviews and an adaptive, principles-based approach are all positive elements of the framework.

We note that the consultation references, in several places, that several major platforms already have Account Compromise and Takeover (ACTO) controls in place. However, the continued prevalence of account takeover and fraudulent advertising suggests that the existence of controls alone should not be regarded as evidence of their effectiveness. Providers should therefore be expected not only to implement controls, but also to assess and demonstrate their effectiveness against defined outcomes, strengthening or adapting them where they are not delivering a meaningful reduction in harm. This will reinforce the importance of outcome-focused regulation, recognising that having controls in place is not synonymous with having controls that are effectively mitigating risk.

However, from a fraud and scams perspective, we believe there are several areas where the proposal could be strengthened.

Greater Emphasis on Intelligence-Led Detection
The proposal focuses primarily on preventative controls such as authentication and access management. Whilst these are important, account takeover is often identified through behavioural indicators rather than authentication failures alone.

We encourage Ofcom to consider explicitly recognising the value of ongoing behavioural monitoring, including indicators such as:

- Unusual changes in advertising activity.
- Sudden increases in advertising spend.
- Password resets followed by high-risk activity.
- Access from new devices, geographies or IP addresses
- Significant changes to account administration or payment details.

These indicators can often provide earlier evidence of compromise than authentication controls alone and can support more effective intervention.

No Explicit Focus on High-Risk Accounts
The proposal applies account security mechanisms to all advertising accounts, which we support. However, it does not explicitly recognise that certain accounts may pose significantly greater fraud risks.

Examples include:

- High-spend advertising accounts.
- Accounts promoting financial products
- Newly created business accounts.
- Accounts linked to previous enforcement activity.
- Accounts displaying unusual behavioural patterns.
- A risk-based approach could enable providers to apply enhanced controls and monitoring where the potential harm is greatest.

Cross-Online Services Threats and Repeat Offending
Member experience indicates that fraudsters operate across multiple Online Services and may seek to compromise or create accounts on several services simultaneously.

The proposals focus largely on individual provider controls and do not address how intelligence relating to compromised accounts, high-risk actors or enforcement actions could be shared across Online Services . Greater collaboration and intelligence sharing could help reduce repeat offending and improve collective resilience. Category 1 online service providers should be required to participate in information sharing arrangements.

Ofcom should clarify the governance of cross-service intelligence sharing, including eligible participants, minimum indicators, permitted purposes, safeguards, acknowledgement and feedback requirements, and arrangements for correcting inaccurate data. Category 1 services should be expected to participate in appropriately governed arrangements for sharing high-confidence indicators linked to banned advertisers, fraudulent domains, repeat infrastructure and account compromise.

Conclusion
UK Finance members support the proposed account security measure and agree that stronger protections against account takeover are critical to reducing fraudulent advertising. However, the framework would be strengthened by:

- Greater use of behavioural and intelligence-led detection.

- Incorporation of confirmed fraud and payment-sector intelligence
- Outcome-based measures of effectiveness.
- More dynamic review and response mechanisms.
- Enhanced controls for higher-risk accounts.
- Stronger consideration of cross-Online Services threats and repeat offending.

These enhancements would help ensure the framework not only protects accounts from unauthorised access but also addresses the broader fraud and scam risks associated with compromised advertising accounts.

Account takeover complaints

UK Finance members support Ofcom's proposal to introduce reporting mechanisms for suspected account takeover and agrees that the rapid identification and remediation of compromised advertising accounts is critical to reducing fraudulent advertising. We particularly welcome Ofcom's recognition that account takeover enables criminals to bypass onboarding, verification and advertiser due diligence controls.

However, we believe the framework could be strengthened in several areas.

Response Times and Service Standards

The proposal requires providers to review reports "promptly" and take action "swiftly" but does not define what these expectations mean in practice. Given the speed at which fraudulent advertising can cause consumer harm, particularly in investment scams and impersonation-based fraud, Ofcom should consider introducing indicative service standards for the review, investigation and remediation of reports.

In particular, where a financial institution notifies an Online Services of fraudulent advertising, impersonation of that institution, or provides credible fraud intelligence, the Codes should require providers to undertake a prompt assessment, maintain clear escalation routes, take appropriate mitigating action where justified, including restriction or removal of content, and provide feedback to the notifying institution on the outcome**.** Defined service standards would help ensure that reports are handled consistently and proportionately, while improving accountability and enabling more effective collaboration between Online Services and the financial sector.

Establishing clearer expectations in this area would help reduce consumer harm, support the rapid disruption of fraudulent activity, and strengthen confidence that reports from trusted sources are being acted upon in a timely and effective manner.

Learning from Account Takeover Incidents

While the proposal focuses on responding to reports, there is less emphasis on learning from account takeover incidents. Where compromised accounts are used to publish fraudulent advertisements, providers should review how the compromise occurred, whether existing controls failed, whether warning signs were missed, and

what enhancements may be required. This would support continuous improvement rather than treating incidents as isolated events.

Proactive Detection
The proposal is largely reactive and dependent on reports being raised. Many account takeovers can be identified proactively through behavioural indicators such as unusual login activity, sudden increases in advertising spend, password resets followed by high-risk behaviour, new device access or significant changes to campaigns and payment details. We encourage Ofcom to place greater emphasis on intelligence-led monitoring and behavioural analytics to reduce reliance on account-holder reporting.

Organised Criminal Activity
The proposal focuses primarily on restoring access to individual accounts. However, account takeover is frequently undertaken by organised criminal groups operating at scale. Compromised accounts often form part of wider campaigns involving multiple accounts, domains, identities and advertisements. Providers should therefore investigate account takeover incidents at both account and campaign level to identify associated activity and prevent broader harm.

Cross-Online Services Intelligence Sharing

UK Finance Members have observed that fraudsters target multiple Online Services using the same infrastructure, credentials and attack methodologies. The proposal does not currently address how intelligence relating to compromised accounts, repeat offenders or emerging fraud typologies could be shared across Online Services. Greater collaboration would improve collective resilience and reduce opportunities for criminals to migrate between services.

Advertising Bans

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

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

UK Finance members support Ofcom's proposal to ban advertisers responsible for fraudulent advertising and to prevent their return to Online Services. We agree that fraud is often perpetrated by organised and financially motivated actors, for whom warnings and graduated sanctions are unlikely to be effective deterrents. However, we believe several areas could be strengthened.

Measuring Effectiveness

The proposal focuses on banning processes but includes limited expectations regarding outcomes.

To support accountability, providers should consider reporting on:

- Repeat offending rates.
- Ban evasion attempts.
- Linked accounts identified.
- Time taken to detect returning bad actors.
- Reductions in fraudulent advertising linked to previously banned advertisers.

Without outcome measures, it may be difficult to assess whether bans are reducing fraud or simply displacing it. Ofcom should require providers to report repeat return rates, linked accounts identified, time to detect re-entry, domains/creatives reused by banned actors, and whether fraudulent advertising linked to previously banned advertisers has reduced.

Stronger Feedback Loops

Where banned advertisers successfully return to an Online Services, providers should review:

- How controls were circumvented.
- Whether onboarding checks were sufficient.
- Whether additional fraud indicators are required.
- Whether detection models require improvement.

This would help ensure enforcement controls continue to evolve alongside criminal methodologies.

Compromised Legitimate Accounts

The proposal references account takeover but could place greater emphasis on the risk posed by compromised legitimate advertisers. As our members observe criminals exploit trusted, verified accounts to bypass controls and distribute fraudulent advertising.

Providers should combine banning controls with enhanced monitoring for account takeover indicators and suspicious account activity.

International Fraud Risks

The proposal focuses on preventing banned advertisers from targeting UK users. However, fraud networks often operate internationally and may use global campaigns and cross-border infrastructure to reach UK consumers.

Ofcom should consider whether broader enforcement measures may be appropriate where Online Services have the capability to prevent wider criminal activity.

Account Appeals

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

UK Finance members support the introduction of account appeal mechanisms and recognise the importance of allowing legitimate advertisers to challenge incorrect decisions. However, the proposals place significant emphasis on advertiser rights and less on ensuring appeals do not weaken fraud prevention outcomes.

Timeliness and Prioritisation
The proposals require appeals to be determined "promptly" but do not provide clear expectations on review times. Ofcom should consider introducing indicative service standards that balance the rights of legitimate advertisers with the need to minimise consumer exposure to fraud and scams. High-risk appeals involving confirmed fraud intelligence, trusted-flagger evidence or linked criminal infrastructure should be prioritised and should not result in reinstatement unless the provider has assessed the full risk context.

Use of Fraud Intelligence
Appeal decisions should not rely solely on information supplied by advertisers. Providers should also consider intelligence from:

- Financial institutions.
- Law enforcement.
- Trusted flaggers, the list of which should be expanded to include specialist in Financial Services illegal harms, such as the Cyber Defence Alliance
- Fraud prevention organisations.
- Scam reports and confirmed fraud intelligence.

This is particularly important where there is evidence of consumer harm or organised criminal activity.

Repeat Offenders and Linked Accounts
The proposals do not explicitly address repeat offending behaviour. Providers should consider linked accounts, associated entities and wider account histories to prevent fraudsters from repeatedly circumventing enforcement through appeals.

Organised Criminal Networks
Fraudulent advertising is often conducted through networks of accounts rather than individual actors. Appeals should be assessed in the context of wider intelligence and associated activity where there is evidence the account forms part of a broader fraudulent operation.

Appeals mechanisms should provide legitimate users and businesses with appropriate opportunities to challenge decisions, while incorporating safeguards to prevent fraudsters from exploiting appeals processes to circumvent Online service controls. Appropriate verification and authentication measures should be embedded throughout the appeals process to ensure that only genuine parties can seek reversals or amendments to enforcement actions. Providers should also monitor and analyse the volume, nature, and outcomes of successful appeals, including the rationale for decisions and any subsequent consumer harm. This information can provide valuable insight into the effectiveness of existing controls, identify potential

weaknesses in enforcement processes, and help determine whether additional safeguards or policy adjustments are required.

4. Moderation

Moderation, Account Integrity and Fraud Prevention

UK Finance members support Ofcom's proposals to strengthen advertising moderation and fraud prevention controls.

Regulatory Oversight and Independent Validation

Members support Ofcom's powers to request transparency reports and conduct audits of Online Services controls. However, given the significance of consumer harm arising from fraudulent advertising, we believe there is value in establishing early and regular oversight of higher-risk Online Services once the new duties come into force.

Independent validation will be essential to demonstrating that controls are operating effectively and consistently across services. Transparency reporting and assurance activities should therefore focus not only on the existence of controls, but on measurable outcomes and their effectiveness in reducing fraud and consumer harm.

Ofcom should also provide greater clarity on accountability and oversight arrangements, including who will assess whether alternative controls deliver equivalent outcomes, who will determine whether providers have met any "reasonable endeavours" obligations, and what level of evidence will be required to demonstrate compliance. Consideration should also be given to the role of independent audit and external scrutiny, particularly where providers continue to exhibit poor outcomes or elevated levels of harm.

A robust, outcome-focused review framework will be critical to ensuring that controls remain effective in practice and that moderation policies evolve alongside criminal methodologies rather than lagging the criminal activity. This approach will help ensure that compliance is assessed not only by the implementation of controls, but by their demonstrable impact in reducing fraud risks and improving consumer protection.

Advertising Moderation

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

Moderation Standards and Trusted Flaggers

Effective Moderation Frameworks

Providers should maintain effective moderation systems supported by clear governance, measurable performance standards and appropriately trained personnel.

Training should incorporate external expertise, including insights from fraud specialists, industry participants and law enforcement, rather than relying solely on internal resources. This will help moderation teams remain responsive to evolving fraud typologies and emerging criminal tactics.

Ofcom should also consider whether moderation performance metrics could form part of transparency reporting requirements.

Trusted Flagger Processes

Members strongly support the use of trusted flagger channels and view them as an important mechanism for rapidly identifying fraudulent content.

However, experiences across Online Services have been inconsistent. We therefore encourage Ofcom to establish clearer expectations regarding:

- Response times for trusted flagger reports.
- Escalation arrangements for high-risk cases.
- Feedback provided to reporting organisations.
- Monitoring of Online Services responsiveness and outcomes.

Trusted reporting frameworks are most effective UK Finance members and trusted intelligence-sharing bodies frequently identify fraudulent content as part of wider investigations involving customer reports, fraud losses, account compromise and criminal infrastructure analysis. These organisations often possess information that would not otherwise be visible to Online Services and are therefore well placed to provide high-confidence indicators of fraud risk. The Online Services must act consistently and transparently on intelligence supplied by recognised experts and industry bodies. Ofcom should therefore require providers to explain rejected trusted-

flagger reports, review repeated rejection patterns, and evidence policy or model changes where rejected reports later correlate with confirmed consumer harm.

Trusted-flagger routes will only be effective if providers are required to act on high-quality fraud intelligence within defined timeframes and can be held accountable where they fail to do so. A provider that has received credible evidence that an advert is fraudulent should not be able to leave that advert live, continue serving impressions or require repeated reporting without a clear explanation. Ofcom should therefore link trusted-flagger performance to supervision, audit and enforcement, including where repeated failures allow the same advertiser, domain, creative or infrastructure to continue causing harm.

Standard Evidence Preservation Requirements

Where fraudulent advertising is suspected or confirmed, providers should immediately preserve relevant artefacts. These should include advert creative, advert and campaign identifiers, advertiser identity information, account history and verification records, landing pages and destination URLs, redirect chains, payment methods used to purchase advertising, moderation decisions, enforcement actions, appeal outcomes, linked accounts, domains and associated infrastructure. Evidence preservation should be triggered by trusted-flagger reports, confirmed fraud intelligence, law-enforcement referrals, regulatory requests or provider-generated indicators of organised criminal activity.

Ad Libraries and Fraud Detection

Members view ad libraries as a potentially valuable fraud prevention tool and support their continued development.

Ad libraries should not operate solely as transparency mechanisms for external stakeholders. Providers should actively utilise them as part of their own moderation, detection and investigative processes to identify emerging fraud trends, repeat offending advertisers and coordinated campaigns.

To maximise effectiveness, Ofcom should require minimum ad-library functionality for in-scope services, including:

- Searchable and filterable interfaces.
- Stable advert, advertiser and campaign IDs.
- Destination URLs, landing pages and redirect chains.
- Enforcement outcomes, removal reasons and appeal history.
- API or bulk access for Ofcom and designated trusted entities.

Retention Periods

We also encourage Ofcom to consider whether the proposed retention periods are sufficient for all fraud typologies. Certain scams, particularly investment fraud and other longer-term frauds, may not be identified or reported until many months or even years after exposure. Certain fraud typologies, including investment fraud and other long-duration scams, may not be identified or reported until a significant period after initial exposure. Ad library retention requirements should therefore be informed by investigative needs, harm timelines and industry evidence to ensure valuable intelligence is not lost prematurely.

We would recommend a five-year retention period.

Scope and Wider Advertising Ecosystem

While we welcome the new duties applying to Category 1 and Category 2A services, it is important to recognise that fraudulent advertising risks extend beyond individual Online Services and are facilitated by a wider ecosystem of advertisers, intermediaries and technology providers.

The Online Safety Act introduces important new protections, but gaps remain within the broader advertising regime. As implementation progresses, Ofcom should continue to assess whether further measures are required to strengthen accountability across the wider advertising supply chain and support more effective prevention of fraud and scam activity and seek to ensure Online Services impose standards and expectations against the wider supply chain. This could include only verified ads being accepted. In addition, the DCMS Online Advertising Taskforce working groups should be monitored for best practice standards and intelligence sharing that can be replicated.

Terms of Service and Publicly Available Statements

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

UK Finance members support the proposed Terms of Service requirements but believes they should place greater emphasis on fraud prevention effectiveness, transparency and continuous improvement. Providers should be encouraged to publish clearer information on fraud controls, enforcement outcomes, treatment of trusted reporter intelligence, repeat offender management and the use of confirmed fraud data. In addition, Terms of Service should be supported by robust feedback mechanisms that ensure policies evolve in response to emerging threats, repeat

reports and evidence of consumer harm. This would help ensure the Online Services policies remain effective against a rapidly changing fraud landscape and contribute to more meaningful reductions in fraud and scam activity.

Advertising Complaints

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

UK Finance members support the introduction of advertising complaints mechanisms and agree that complaints are an important source of intelligence regarding fraudulent advertising. However, the proposals place greater emphasis on enabling complaints to be submitted than on ensuring that complaints systems deliver effective fraud prevention outcomes.

We encourage Ofcom to strengthen the framework through clearer response expectations, enhanced treatment of trusted reporters, stronger feedback loops, the effective use of confirmed fraud intelligence, aggregation of related reports, and outcome-based performance measures. These enhancements would help ensure that complaints mechanisms contribute not only to content review, but also to the ongoing detection, disruption, and prevention of fraud and scams.

Consumer Exposure Notifications

Where a provider determines that a fraudulent advertisement has been served to users, it should assess whether affected users can be notified through proportionate means such as in-app alerts, account notifications, warning messages or other customer communications. The objective should not only be removal of harmful content but reduction of ongoing consumer exposure and earlier intervention before losses occur. Providers should retain sufficient records to identify whether users interacted with, clicked on or were exposed to fraudulent advertising so that notifications can be targeted appropriately and audited by Ofcom.

Notifications should explain clearly that the user may have encountered a fraudulent advert, identify the relevant interaction where appropriate, recommend proportionate protective action and signpost users to suitable reporting or support routes. Providers should measure whether notifications are timely, targeted and effective in reducing further harm.

Advertising Appeals Are Stronger Than Fraud Escalation
The proposal contains considerable detail regarding advertiser appeals and procedural fairness.

While this is important, there appears to be less detail regarding:

- Victim protection.

- Fraud escalation.
- High-severity scam reporting.

In addition, Ofcom should ensure that advertising complaints channels are clearly scoped and do not evolve into general-purpose or "super-complaint" mechanisms. Providers should be required to collect structured information on the reason for a complaint and clearly communicate that these channels are intended for reporting suspected fraudulent advertising, rather than wider advertising disputes that may be more appropriately directed to organisations such as the ASA or FCA. Without clear guardrails, complaints systems risk becoming overwhelmed by volume and noise, undermining the objective of swift fraud handling and potentially resulting in inconsistent and costly outcomes across Online Services.

Fraud Concern
The framework currently provides clearer routes for advertisers to challenge decisions than for fraud experts, trusted reporters, or victims to escalate harmful content. Ofcom should ensure fraud escalation routes are at least as clear, timely and accountable as advertiser appeal routes, particularly for high-severity scams and trusted-flagger reports. Greater emphasis should be placed on ensuring that legitimate fraud concerns can be raised, assessed, prioritised, and acted upon quickly, while maintaining appropriate controls to prevent complaints channels from becoming a de facto mechanism for resolving general advertising disputes. This would help Online Services focus resources on the timely identification and removal of fraudulent advertising and reduce the risk of consumer harm.

Ad Libraries

Do you agree with our proposal?

Please provide any arguments and supporting evidence.

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.

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?

Members strongly support the principle of ad libraries and recognise their potential to become a powerful tool for identifying fraudulent advertisements, investigating threat actors, protecting consumers from impersonation scams, and supporting broader

disruption activity. However, current usage varies significantly across firms. While some organisations have developed mature, intelligence-led capabilities, others face challenges relating to access, functionality, resourcing, and the integration of ad library intelligence into operational fraud processes.

There is a clear and consistent view across members that ad libraries should evolve beyond their current role as transparency mechanisms and become more effective operational tools for fraud prevention. To support this, Online Services should provide richer datasets, enhanced search and analytical functionality, improved access arrangements for trusted stakeholders, and clearer mechanisms for acting on intelligence and removing harmful content. Ad libraries should also play a more prominent role within Online Services ' own fraud detection and moderation frameworks, supporting the identification of repeat offenders, coordinated fraudulent activity, emerging threats, and campaigns associated with consumer harm.

To realise this potential, Ofcom should require Online Services to provide richer datasets, enhanced search and analytical functionality, improved access for trusted organisations, and effective mechanisms for actioning intelligence and removing fraudulent content. Ad libraries should also play a central role in Online Services ' own moderation and detection processes, helping to identify repeat offenders, emerging threats and harmful campaigns before they result in consumer harm

At the same time, UK Finance recognises that not all information contained within ad libraries can or should be made publicly available. Certain data may be commercially sensitive, security-sensitive, or subject to legitimate privacy and data protection considerations. Ofcom should therefore distinguish between information that should be publicly searchable to support transparency and consumer confidence, and information that should be accessible only to trusted organisations, regulators, law enforcement agencies, and other authorised parties for the purposes of fraud prevention, investigation, and disruption.

A tiered-access approach would help balance transparency with appropriate safeguards. Publicly accessible information can promote accountability and informed consumer decision-making, while enhanced access for trusted stakeholders would enable more effective fraud detection, investigation, and enforcement activity. Such an approach would protect legitimate advertisers from unnecessary disclosure of sensitive information, remain consistent with data protection principles, and ensure that those with a legitimate role in tackling fraud have access to the intelligence needed to identify and disrupt criminal activity. This would strengthen the overall effectiveness of ad libraries as both a transparency mechanism and a practical tool for preventing consumer harm.

Current Use Across Industry

Member responses demonstrate three broad levels of maturity below, in the current environment. These examples should be used to help identify the capabilities and outcomes that may be required; however, it should remain for Online Services to determine how best to incorporate them into the design and operation of their own systems and controls

- Some firms do not currently use ad libraries due to a lack of tools, resource, or established fraud investigation processes.
- Some firms use ad libraries periodically or on an ad hoc basis following customer reports, intelligence leads or brand impersonation concerns.
- More advanced users regard ad libraries as a key cyber-fraud intelligence source and use them daily to identify fraudulent campaigns, brand impersonation, investment scams, fake customer support pages, wallet provisioning fraud and wider social engineering threats.

Meta's Ad Library was cited by our members as the most useful current capability due to its functionality, searchability and ability to pivot across adverts, businesses and associated profiles. Other ad libraries were generally viewed as providing more limited datasets and functionality

Key Benefits Identified

Members highlighted that ad libraries can support:

- Detection of brand impersonation and fraudulent use of financial services brands.
- Identification of scam campaigns targeting customers.
- Investigation of wider criminal infrastructure and threat actor activity.
- Discovery of related advertisements and connected fraudulent profiles.
- Intelligence gathering to support customer warnings and awareness campaigns.
- Referral and takedown activity through initiatives such as the Cyber Defence Alliance (CDA).

More sophisticated users have highlighted the value of ad libraries in clustering criminal campaigns, identifying malicious domains, mapping fraud ecosystems and feeding intelligence into wider disruption activities.

Minimum Requirements for Effective Ad Libraries

Members identified a consistent set of features required for ad libraries to support fraud prevention effectively:

- Stable advertiser, page and account identifiers.
- Advertiser attribution and verified business information.

- Full advertisement content, including images, videos and text.
- Visibility of landing pages, destination URLs and redirect chains.
- Account history and profile creation dates.
- Advertisement duration and delivery timelines.
- Enforcement and moderation outcomes.
- Searchable and filterable interfaces.
- API and bulk export functionality to support automation and analytics.

The ad libraries should support both manual investigations and automated fraud detection workflows. Our members have identified several enhancements that would significantly increase the value of ad libraries:

Attribution and Provenance

- Verified advertiser identities and KYC information.
- Historical account and advertiser name changes.
- Stable advertiser and campaign identifiers.
- Cross-Online Services and cross-surface advertisement tracking.

Creative and Infrastructure Intelligence

- Downloadable copies of advertisement creatives.
- Creative hashes to identify duplicate and modified advertisements.
- Full destination URL chains and redirects.
- Associated domains, infrastructure and contact details.
- Visibility of embedded phone numbers and email addresses.

Delivery and Audience Information

- Advertisement approval and delivery timestamps.
- Geographic reach data.
- Audience targeting categories.
- Impression and spend ranges.

Enforcement and Transparency

- Moderation outcomes and policy violation categories.
- Enforcement action details.
- Warning, suspension and ban data.
- Appeal histories and audit trails.

Integration and Automation

- Bulk export capabilities.
- APIs and webhooks.
- Stable schemas and technical documentation.

- Integration with trusted reporter and fraud referral schemes.

Common Challenges and Limitations

We welcome the requirement that the Online Services provide ad libraries as Members raised several concerns regarding current ad library capabilities:

- Limited availability of data across some Online Services.
- Inability to report inactive advertisements, despite evidence that threat actors frequently deactivate and subsequently reactivate campaigns.
- Reliance on users already knowing what to search for.
- Lack of indexing by fraud type, geography or industry sector.
- Limited transparency regarding advertiser activity and enforcement history.
- Difficulty identifying personalised or dynamic fraudulent advertising.

Online Services Responsiveness

A consistent theme was concern regarding Online Services responsiveness. Members reported:

- Low and inconsistent takedown rates from online services.
- Reports of impersonation content not always resulting in action.
- Similar fraudulent content often remaining active despite repeated reporting.
- Limited visibility of outcomes following referrals.
- Several members stressed that ad libraries should not simply be transparency tools for external stakeholders. Online Services themselves should actively use these datasets to identify fraudulent activity, detect repeat offenders and improve moderation effectiveness.

The responsiveness of Online Services should be linked to measurable service levels and Ofcom supervision. Providers should report trusted-flagger acceptance rates, rejection rates, median response times, removal rates, recurrence rates and reasons for no action, so Ofcom can identify inconsistent or ineffective response practices.

Key Implementation Requirements for Ofcom

- Stronger Online Services accountability for identifying and removing fraudulent advertisements.
- Continuous monitoring and validation of advertisements throughout their lifecycle.
- Enhanced transparency around moderation decisions and enforcement outcomes.
- Faster responses to reports from trusted entities.
- Better search, analytical and investigative capabilities within ad libraries.

- Bulk access, APIs and automation functionality.
- Intelligence-sharing mechanisms that support collaboration between Online Services, financial institutions and trusted reporters.
- Longer-term retention and accessibility of advertising data to support investigations and trend analysis.
- Greater use of ad libraries by Online Services themselves, rather than relying primarily on external reporting to identify fraud.

The reason these requirements are necessary is straightforward: banks, consumers and trusted reporters often identify the harm downstream, after the advert has disappeared or the consumer has moved off platform. Member experience demonstrates that investigations are frequently hindered by the absence of historical advertising data, incomplete advertiser attribution and limited visibility of linked campaigns. This can delay disruption activity, reduce opportunities to identify additional victims and make it more difficult to establish patterns of criminal behaviour. Enhanced ad-library capabilities would address a number of these practical investigative challenges. Platforms are best placed to preserve the upstream evidence and disrupt the advertising infrastructure before further users are exposed. Making ad libraries operational, durable and accessible therefore supports prevention

Ad libraries also provide an important check on commercial incentives within the advertising ecosystem. Where a provider has monetised an advert, it should be able to preserve and disclose the core information needed to understand who paid for it, how it was targeted, where it directed users, what action was taken and whether similar activity reappeared. Without durable advert, advertiser, payment-route and enforcement data, it is difficult for Ofcom or trusted entities to assess whether platforms are genuinely disrupting fraudulent advertising or merely removing individual adverts after harm has occurred.

Overall Industry Position

Members strongly support the principle of ad libraries and see significant value in their further development. However, there is a clear view that ad libraries should evolve beyond transparency mechanisms into operational fraud prevention tools that support proactive detection, intelligence sharing, advertiser accountability, campaign disruption and consumer protection. Ofcom should specify the minimum data fields, access mechanisms, retention period, preservation triggers and reporting obligations required for ad libraries to function as fraud prevention infrastructure, not simply public transparency tools.