Fighting Economic Crime Together

Cifas response to Consultation

Fraudulent Advertising Codes

About Cifas

Cifas is the UK's fraud prevention service. Our purpose is to keep people and organisations safe from fraud and scams.

We are a not-for-profit membership organisation with over 800 Members across twenty-five key sectors including financial services, retail, insurance, telecommunications, technology and the public sector. We enable the sharing of critical data and intelligence across the public, private and third sectors to help protect people and businesses from the harm caused by fraud.

Cifas operates the National Fraud Database, the largest holding of cross-sector fraud-risk data in the UK. In 2025, Cifas enabled its Members to prevent more than £2.4 billion in fraud losses.

Introduction

Cifas welcomes Ofcom's proposed Fraudulent Advertising Codes and broadly supports the prevention-led, layered approach set out in the consultation. Fraudulent advertising is an adversarial and evolving threat. Effective action therefore requires more than removal of individual advertisements after harm has occurred. Strong account integrity, dynamic fraud-risk assessment, effective moderation and specialist reporting routes should operate together to prevent fraudulent actors gaining access to advertising systems, identify emerging risk and enable swift disruption.

Cifas's principal recommendations are that Ofcom should:

- Retain the strong preventative and account-integrity focus of the Codes;
- Ensure fraud indicator assessments can draw on high-quality external and cross-sector fraud data and intelligence;
- Provide an effective route for expert fraud-prevention organisations to participate in trusted-flagger arrangements;
- Ensure controls remain responsive to criminal adaptation and displacement; and
- Evaluate the Codes through measurable fraud-prevention outcomes as well as procedural compliance.

Cifas's 2026 fraud-risk evidence provides relevant context. More than 220,000 cases were filed to the National Fraud Database in the first six months of 2026. Identity fraud accounted for 59% of filings and facility takeover increased by 5%.[1] These data do not establish that the recorded cases originated from fraudulent advertising. They demonstrate the wider identity, account-compromise and criminal-adaptation environment in which the Codes will operate.

[1] Fraudscape 2026: 6 Month Update. https://www.fraudscape.co.uk/

Volume 1: Context

Q1. Is there any information or evidence that could enhance Ofcom's understanding of the online advertising ecosystem?

Cifas agrees with Ofcom that the online advertising ecosystem should be understood as a complex system in which responsibility and relevant information may be distributed across service providers, advertisers and intermediaries.

From a fraud-prevention perspective, we encourage Ofcom to consider the advertising ecosystem as one component of a wider fraud ecosystem. Relevant risk information may arise outside the immediate advertising pathway, including information relating to compromised identities, accounts, contact details, payment information, domains and other signals associated with previous fraud.

Cifas therefore considers that effective controls should enable providers, where lawful, necessary and proportionate, to make appropriate use of reliable external fraud-risk information. Complexity in the supply chain should not create gaps through which responsibility for preventing fraud can fall.

Q2. Do you have any comments on Ofcom's assessment of the causes and impacts of fraudulent advertising?

Cifas broadly agrees with Ofcom's assessment, particularly its recognition that fraudulent advertising is highly adversarial and that perpetrators change tactics to evade detection.

We recommend that Ofcom give additional prominence to criminal adaptation and displacement when evaluating the Codes. Reducing fraudulent advertising through one account type, service or advertising pathway does not necessarily remove criminal intent or capability. Fraudsters may change identities, accounts, channels or methodologies in response to intervention.

Cifas's latest fraud-risk data illustrates this wider adaptive environment. In the first half of 2026, more than 220,000 cases were filed to the National Fraud Database. Identity fraud accounted for 59% of filings and facility takeover increased by 5%. These figures should not be interpreted as quantifying fraudulent advertising. They demonstrate the wider fraud environment in which the proposed controls will operate. [2]

These figures should not be interpreted as quantifying fraud caused by the specific vulnerabilities considered by this Call for Evidence. Cifas does not currently hold evidence allowing that attribution to be made.

We encourage the Government with Ofcom to develop more granular evidence base capable of linking particular vulnerabilities to harm resulting in fraud. This would support both the targeting of intervention and subsequent evaluation of whether measures are effective.

[2] Fraudscape 2026: 6 Month Update. https://www.fraudscape.co.uk/

Q3. Do you agree with Ofcom's examples of risky characteristics?

Cifas agrees with Ofcom's proposed examples of risky characteristics and supports their use as part of a wider, dynamic assessment of fraudulent-advertising risk.

We particularly support Ofcom's focus on impersonation, suspicious advertising-account behaviour and the use of generative AI and deepfakes. These characteristics are especially relevant to Cifas's wider experience of identity fraud, account compromise and increasingly sophisticated digitally enabled fraud. Cifas's latest fraud-risk data shows that identity fraud remains the largest category of cases filed to the National Fraud Database, accounting for 59% of filings in the first six months of 2026, while facility takeover increased by 5%. Cifas's analysis also identifies AI-enabled scams, compromised personal information and account compromise as features of the evolving fraud threat.[3]

Impersonation is particularly important because criminals can exploit the identity, brand or reputation of a legitimate individual or organisation to give fraudulent activity an appearance of credibility. We therefore support Ofcom treating impersonation of brands, organisations and public figures as a relevant indicator of risk.

We also support Ofcom's focus on suspicious advertising-account behaviour. Account-level changes and behavioural signals can provide an important opportunity to identify risk before or alongside assessment of an individual advertisement. This is consistent with the wider Cifas view that fraud prevention should seek to intervene as early as possible and make use of relevant fraud-risk information rather than relying exclusively on action after harm has occurred. Cifas has previously advocated prevention before harm and earlier identification of fraud risk through high-quality data and intelligence.

Finally, Cifas supports the inclusion of generative AI and deepfakes as a risky characteristic. Their significance lies not solely in the technology itself, but in the potential for these tools to make impersonation and other forms of deceptive content more convincing and scalable. Cifas's 2026 fraud analysis identifies increasingly sophisticated AI-enabled scams as part of the wider evolving fraud environment.

However, Cifas would caution against treating any of these characteristics as definitive evidence of fraud when viewed in isolation. Legitimate advertising may display individual characteristics also associated with fraudulent activity, while sophisticated criminals will adapt as particular indicators become better understood.

We therefore support an approach in which risky characteristics are considered individually and in combination with other relevant signals, including account behaviour and reliable external fraud intelligence. The framework should also remain sufficiently dynamic to incorporate emerging indicators as criminal methodologies change.

Q4. Do you agree with Ofcom's proposed overall approach to the Codes?

Cifas supports Ofcom's layered and safety-by-design approach.

[3] Fraudscape 2026: 6 Month Update. https://www.fraudscape.co.uk/

No single intervention will adequately address fraudulent advertising. Prevention should begin before harmful advertisements reach consumers, particularly through account integrity, verification and risk assessment, and be reinforced by detection, moderation, reporting and effective action after suspicious activity is identified.

Cifas particularly supports the emphasis on prevention before harm. We also recommend that Ofcom evaluate the package as a connected system and monitor whether criminal activity is displaced to other services, channels or advertising pathways.

Q5. Do you consider the overall burden on service providers to be proportionate?

Cifas considers the overall burden created by the proposed measures to be proportionate to the seriousness and potential impact of fraudulent advertising.

In considering proportionality, it is important that the costs and operational requirements placed upon service providers are considered alongside the potentially significant harm experienced by consumers and legitimate businesses when fraudulent advertising is allowed to reach users. Cifas has consistently supported stronger measures to prevent fraudulent online advertising and has previously highlighted the harm it can cause to consumers, businesses and particularly vulnerable individuals. Cifas welcomes plans for legislation to combat fraudulent advertising

There is also an important qualitative distinction between fraudulent advertising and some other forms of unsolicited criminal communication. Paid advertising presented through an established online platform can potentially provide the initial approach made by a fraudster with an appearance of legitimacy. In Cifas's view, this can be particularly concerning where the advertisement is the starting point for subsequent social engineering.

Once an individual responds to or acts upon fraudulent advertising, the interaction may move beyond the platform into other channels where the fraudster can employ social-engineering techniques. Cifas's fraud evidence demonstrates the wider significance of social engineering, with Cifas Members reporting concerns about criminals using increasingly sophisticated techniques, including AI and deepfake technology, to obtain personal information, steal identities and compromise accounts. [4]

The preventative value of the Codes should therefore be considered not simply in terms of removing a misleading advertisement, but in disrupting a potential entry point into a wider fraud journey. Where fraudulent advertising provides the initial credibility needed to establish contact, allowing that advertisement to reach a consumer may create an opportunity for subsequent manipulation and social engineering.

This reinforces the importance of intervention before exposure wherever reasonably possible. Requiring consumers to identify sophisticated fraudulent advertisements themselves or relying predominantly on removal after an advertisement has been reported, risks placing too much responsibility on the potential victim once the opportunity for the fraudster to establish contact has already arisen.

[4] Fraudscape 2026: 6 Month Update. https://www.fraudscape.co.uk/

Cifas recognises that the measures will create implementation and operational costs for providers. Requirements should therefore remain risk-based and should avoid unnecessary friction for legitimate advertisers. However, proportionality should be assessed against the harm prevented as well as the cost of prevention. In Cifas's view, the potentially serious consequences of fraudulent advertising justify robust preventative measures, provided those measures are properly targeted and demonstrably effective.

Volume 2: Risk, governance and control

Q6. Do you agree with Ofcom's proposal for providers using advertising intermediaries?

Cifas supports the principle that the use of an advertising intermediary should not result in materially weaker fraud-prevention outcomes.

The proposed "all reasonable endeavours" approach can provide necessary flexibility where a provider genuinely lacks control over part of the advertising pathway. However, flexibility should not create a weakest-link problem in which responsibility is repeatedly transferred along the supply chain.

We support Ofcom's proposed record-keeping around measures a provider cannot implement, the reasons why and the alternative steps taken. Providers should also be able to demonstrate whether those alternative arrangements produce comparable safety outcomes.

Q7. Do you have comments or additional examples concerning "all reasonable endeavours" and advertising intermediaries?

Cifas supports Ofcom's examples of working with or requiring intermediaries to undertake moderation or account checks where the provider cannot do so directly.

As a further principle, arrangements should ensure that actionable fraud-risk information can move to the organisation in the chain capable of preventing or disrupting the activity. The objective should not be to maximise the volume of information exchanged, but to ensure relevant, accurate and timely information reaches the organisation able to act.

Providers should maintain clear accountability for the outcome, including where a control is delivered contractually by an intermediary.

Q8. Do you agree with the proposed fraud indicator assessment?

Cifas strongly supports the proposed fraud indicator assessment.

Fraud is adversarial. The characteristics associated with fraudulent activity change as criminals learn how controls operate. Providers should therefore identify combinations of indicators, track emerging characteristics and refresh assessments as threats evolve.

The assessment should inform preventative interventions as well as post-event detection. We support Ofcom's proposal that the assessment be connected to other mitigations across the Codes.

Q9. Are there other information sources providers should consider when assessing how fraudulent advertising manifests?

Cifas considers that providers should, where relevant and lawfully available, draw on high-quality external fraud-risk data and intelligence alongside information generated on their own services. No individual organisation will necessarily see the entirety of a fraud journey, and information generated across other sectors can provide important indicators of identities, accounts, infrastructure and methodologies associated with fraudulent activity.

The National Fraud Database (NFD) provides an example of the value of cross-sector fraud-risk information. The NFD holds fraud-risk data relating to identity fraud, facility takeover, false applications, misuse of facility and other forms of fraudulent conduct. It also enables connections between cases sharing common data elements to be identified through network analysis and incorporates intelligence from trusted third-party sources.

This type of cross-sector information can complement the information visible to an individual online service. A provider's understanding of potentially fraudulent activity should not necessarily be limited to the content of an advertisement or activity occurring solely within its own platform. Where appropriate legal, security and governance safeguards are in place, relevant external fraud-risk information may provide additional context capable of strengthening an assessment of risk.

Cifas's Scamlink initiative provides a further example particularly relevant to online scams. Scamlink enables participating organisations to submit scam-related signals including malicious URLs, IP addresses, domain names, email addresses, telephone numbers and social media handles. These signals can then be routed to trusted external partners for potential disruption of scam infrastructure.

Signals of this kind could be particularly relevant to a fraud indicator assessment. For example, information associating a URL, domain or social media handle with reported scam activity could provide additional context when considered alongside indicators identified by a provider within its own service. Intelligence concerning connected infrastructure could also assist providers in considering whether an individual advertisement forms part of wider linked activity.

Providers should also consider strategic and emerging-threat intelligence, rather than relying solely on known indicators derived from historic incidents. Cifas's Fraudscape Report combines National Fraud Database data with intelligence from Cifas Members and key partners to identify cross-sector fraud trends and changes in criminal tactics. The latest analysis highlights the continued exploitation of compromised personal and account information, advancing social-engineering tactics and the increasing sophistication of AI-enabled scams, and emphasises the importance of cross-sector collaboration and data and intelligence sharing in responding to evolving criminal methodologies.

Cifas therefore recommends that Ofcom explicitly recognises three complementary forms of external information that providers could consider as part of their fraud indicator assessments:

- **Cross-sector fraud-risk data** - providing additional context around identities, accounts and previous fraudulent conduct;
- **Actionable scam signals** - including malicious URLs, domains, IP addresses, email addresses, telephone numbers and social media handles; and

- **Strategic fraud intelligence** - identifying emerging methodologies, changing criminal behaviour and indicators that may not yet be apparent from a provider's own historical information.

The governing principle should remain purposeful and proportionate information sharing. External information should contribute to a defined fraud-prevention or disruption outcome and be subject to appropriate standards of quality, accuracy, privacy, security and governance. It should form part of a wider assessment of risk rather than, in isolation, automatically determining that an advertisement, account or individual is fraudulent.

Q10. Do you agree with Ofcom's governance and accountability proposals?

Cifas supports Ofcom's governance proposals, including senior oversight, clear accountability, responsibility statements, independent monitoring and assurance, standards of conduct and appropriate training.

Fraud prevention should be treated as an organisational responsibility rather than solely as a moderation function. Governance bodies should understand whether controls are preventing harm, how criminals are adapting, whether false positives are arising and whether risks are migrating elsewhere.

Cifas recommends that assurance focus on the effectiveness of controls as well as evidence that required processes exist.

Q11. Do you agree with the proposal to test advertisement-generation tools?

Cifas supports the proposal that providers test advertisement-generation tools for ways in which they could be exploited to create fraudulent advertising.

Testing should reflect adversarial misuse and should be repeated as technology and criminal methods evolve. Findings from real-world incidents and emerging fraud intelligence should inform future testing and mitigation.

Cifas's wider fraud analysis highlights the growing relevance of AI-enabled scams and digitally manipulated material. This evidence provides context for the threat but does not demonstrate that platform advertising-generation tools caused the cases recorded by Cifas.

Volume 3: Ensuring account integrity

Q12. Do you agree with Ofcom's proposed account checks and actions, including checks (a) to (d)?

Cifas strongly supports the proposed account checks and actions framework.

On (a), verifying that an advertising account holder genuinely works for or acts on behalf of the person or organisation being advertised is an important preventative control against impersonation.

On (b), controls should seek to prevent banned advertisers returning through new or existing accounts. Action against a single account is unlikely to provide durable disruption if the same actor can readily re-enter.

On (c), Cifas supports proportionate restrictions where account-level indicators demonstrate a material risk of fraudulent advertising, with appropriate review and appeal safeguards.

On (d), Cifas strongly supports repeat checks. Verification should not create permanent trust in an account. Relevant changes in account behaviour, control or risk should be capable of triggering renewed scrutiny.

Q13. Are there other account checks and actions providers could undertake?

Cifas recommends that Ofcom explicitly recognise the value of appropriate cross-account and cross-sector fraud-risk analysis.

Fraudsters may alter individual attributes while retaining links to previous fraudulent activity. Providers should therefore be capable of considering combinations of relevant information rather than viewing each new account in isolation.

Where lawful, necessary and proportionate, reliable external fraud intelligence should be capable of triggering enhanced scrutiny. We do not recommend adding a single universal check for all accounts where the evidence does not demonstrate that such a check would be proportionate.

Q14. Do you agree with the proposed financial services verification policy?

Cifas supports the proposal that providers verify that individuals and firms advertising financial services have the appropriate legal permissions before advertisements can be encountered by UK users.

Upstream verification is preferable to relying solely on remediation once consumers have been exposed to fraudulent financial promotions.

Checks should remain robust to impersonation. Confirmation that an authorised firm exists should not by itself demonstrate that the account placing an advertisement is genuinely acting for that firm.

Q15. Do you agree with Ofcom's proposals for countering advertising-account takeover?

Cifas strongly supports both an effective account-security mechanism and an accessible mechanism for reporting suspected account takeover.

Cifas's wider evidence demonstrates the continuing importance of account compromise. Facility takeover filings increased by 5% in the first half of 2026. This is not a measure of advertising-account takeover, but it supports the broader case for treating compromised accounts as a significant fraud-enabling risk. [5]

Where a credible takeover report is received, providers should be able to assess and contain the risk swiftly while preserving appropriate safeguards for legitimate account holders.

[5] Fraudscape 2026: 6 Month Update. https://www.fraudscape.co.uk/

Q16. Do you have evidence about the frequency or impact of advertising-account takeover?

Cifas does not currently hold evidence that enables us to quantify advertising-account takeover specifically.

We can provide wider contextual evidence. Cifas recorded 39,878 facility takeover cases in the first six months of 2026, an increase of 5% compared with the corresponding period in 2025.[6] This demonstrates the continuing significance of account compromise across the wider fraud landscape.

These data should not be interpreted as quantifying advertising-account takeover or establishing that the recorded cases involved online advertising. We encourage Ofcom to continue developing an evidence base specific to advertising accounts.

Q17. Do you agree with Ofcom's advertising-ban proposal?

Cifas supports the principle that advertising account holders found to have posted fraudulent advertisements should be prevented from simply continuing the activity through the same service.

Effective controls should address repeat behaviour and circumvention, rather than treating removal of an individual advertisement or closure of one account as the end of the intervention. However, Cifas considers that this principle should also extend beyond the boundaries of an individual platform. Preventing a fraudulent advertiser from returning to one service will have limited wider preventative value if the same actor can simply migrate to another platform and continue the same activity.

Cifas therefore recommends that Ofcom considers how appropriate information about confirmed fraudulent advertisers, associated identifiers and relevant fraud signals could be shared securely between platforms through an appropriately governed, neutral intermediary. The purpose should be to enable other providers to identify potential repeat or displaced activity and undertake their own proportionate assessment, rather than automatically imposing an adverse decision solely on the basis of information supplied by another platform.

There are existing models which demonstrate the potential value of collaborative signal sharing. Cifas's Scamlink initiative provides a centralised mechanism through which scam-related signals, including URLs, IP addresses, domain names, email addresses, telephone numbers and social media handles, can be collected and shared with external partners to support disruption.

A neutral or appropriately governed third-party mechanism could support consistent standards around data quality, verification, security and appropriate information sharing, while reducing reliance on multiple bilateral arrangements between individual providers. The objective should be collective prevention, ensuring that action against fraudulent activity identified on one platform can, where appropriate, contribute to the wider ecosystem's ability to identify and disrupt attempts to re-establish that activity elsewhere.

Any such arrangement would require appropriate safeguards. Shared information should be sufficiently reliable and relevant, its use should be proportionate, and providers should undertake

[6] Fraudscape 2026: 6 Month Update. https://www.fraudscape.co.uk/

their own assessment before taking adverse action. The controls should also sit alongside effective complaints and appeals mechanisms for legitimate advertisers who have been incorrectly associated with fraudulent activity.

Without an appropriate mechanism for cross-platform intelligence sharing, Cifas considers there is a risk that otherwise effective advertising bans could displace fraudulent activity between services rather than achieve meaningful disruption of the underlying threat.

Q18. Are there additional circumstances in which an advertising ban should be reversed?

Cifas has not identified evidence supporting additional broad circumstances in which an advertising ban should automatically be reversed beyond those identified by Ofcom. We would caution against creating broad or predictable exceptions that could be exploited by fraudulent actors to circumvent controls and regain access to advertising services.

However, Cifas considers it important that an advertising ban can be reversed where subsequent evidence demonstrates that the original decision was incorrect, materially unreliable or applied to the wrong advertising account holder. Ofcom's proposed arrangements recognise this principle by allowing an account holder to dispute a ban they believe has been applied to the incorrect account holder and, where that appeal is upheld, requiring the provider to reverse the original decision and consider whether the ban should more appropriately apply elsewhere.

Cifas's own approach to fraud-risk information provides a relevant parallel. The National Fraud Database framework requires Cifas Members to investigate complaints relating to cases held on the NFD in accordance with the Cifas complaints policy, recognising that individuals have the right to challenge information they believe to be incorrect.

Cifas therefore considers that effective fraud prevention and procedural fairness should operate together. Providers should be able to take decisive action where fraudulent activity is sufficiently established, while retaining the ability to correct that action where subsequent evidence demonstrates that the original decision was wrong.

Any additional grounds for reversing a ban should therefore be clearly defined, evidence-based and auditable, ensuring legitimate account holders have effective redress without creating easily exploitable routes through which fraudulent actors can circumvent otherwise appropriate restrictions.

Q19. Do you agree with Ofcom's proposed account-appeal arrangements?

Cifas supports Ofcom's proposed account-appeal arrangements. Strong preventative controls should be accompanied by a fair, transparent, accessible and timely mechanism through which legitimate account holders can challenge an adverse decision.

We welcome Ofcom's proposal that account holders should be able to appeal action resulting from failed account checks, failed financial-services checks and other checks undertaken under a provider's account checks and actions policy, and that providers should determine those appeals promptly. Where an appeal is upheld, Ofcom proposes appropriate remedial action, including reversing restrictions and restoring relevant advertising functionality.

This principle is consistent with Cifas's own approach to the National Fraud Database. Cifas Members are required to investigate complaints concerning NFD cases, while the NFD framework requires information used to support risk-based decisions to be interpreted proportionately. The framework also provides that a member must not reject or withdraw a product solely on the basis of an NFD match or alert without undertaking an investigation.

Cifas considers that a similar principle should underpin Ofcom's approach. The identification of a fraud-risk indicator should support appropriate assessment rather than automatically result in an irreversible adverse outcome. Legitimate advertisers should have a meaningful opportunity to provide relevant evidence and seek correction where they believe a decision has been made incorrectly.

An effective appeals process can also contribute to improving the underlying fraud controls. Ofcom proposes that, where there is a pattern or significant evidence of advertisements being removed in error, providers should adjust relevant internal advertising policies and take steps to prevent automated moderation systems from incorrectly removing the same advertisement again.

Cifas supports this feedback principle. Providers should use the outcomes of complaints and appeals not only to correct individual decisions but, where appropriate, to identify recurring weaknesses in risk indicators, data quality or decision-making processes.

Overall, Cifas considers that robust fraud prevention and an effective appeals process are complementary rather than competing objectives. Strong controls should enable decisive intervention where fraud risk is substantiated, while transparent and proportionate appeals provide necessary protection against erroneous decisions and can help improve the effectiveness of the control environment over time.

Volume 4: Moderation

Q20. Do you agree with Ofcom's advertising-moderation proposals?

Cifas supports the proposed moderation framework, while emphasising that moderation should complement rather than substitute preventative controls.

Providers should have effective systems for reviewing suspected fraudulent advertisements and taking swift action when fraud is identified. Prioritisation should be informed by risk and available fraud intelligence.

Where a suspicious advertisement appears linked to wider activity, providers should consider whether the signal identifies other related advertisements, accounts or infrastructure. Effective disruption should seek to address recurring activity rather than only the individual reported asset.

Q21. Do you agree with the proposals on terms of service and publicly available statements?

Cifas supports appropriate transparency regarding providers' use of proactive technology for fraudulent-advertising compliance.

Transparency should give users, advertisers and regulators meaningful information about how risk is managed, while avoiding the disclosure of operational detail at a level that materially assists criminals to circumvent detection systems.

The final balance should therefore support accountability without turning fraud-prevention controls into a predictable checklist for adversarial actors.

Q22. Do you agree with Ofcom's proposals for advertising complaints and dedicated reporting channels?

Cifas strongly supports Ofcom's proposals for dedicated reporting channels for trusted flaggers. However, the effectiveness of these arrangements will depend not only on the existence of those channels, but on ensuring that the trusted-flagger ecosystem is sufficiently broad to capture the high-quality fraud data, intelligence and expertise held across the wider fraud-prevention ecosystem.

Fraud is inherently cross-sector. No single organisation sees the entirety of a fraud journey, and no individual provider can reasonably expect to identify and disrupt fraudulent advertising using its own information alone. Cifas's approach to fraud prevention is founded on collaboration and the sharing of critical data and intelligence across sectors. The collective view created by pooling information can identify threats and patterns that may not be visible to organisations operating in isolation.

Trusted flaggers therefore have the potential to provide an important bridge between intelligence held across the wider fraud-prevention ecosystem and the online providers capable of taking action against fraudulent advertising. Ofcom itself recognises trusted flaggers as expert organisations using specialised reporting routes to report suspected fraudulent advertisements and identifies trusted flaggers as one means through which providers may be alerted to potentially fraudulent advertising.

Cifas is well placed to demonstrate the potential value of this model. We operate the National Fraud Database, the UK's largest holding of cross-sector fraud-risk data and enable the sharing of critical data and intelligence across public, private and third-sector organisations. Cifas also brings together intelligence contributed by professionals across sectors, government and law enforcement.

Alongside these established data holdings, Cifas's Scamlink initiative demonstrates the potential value of sharing actionable scam intelligence. Scamlink enables participating organisations to submit scam-related signals including malicious URLs, IP addresses, domain names, email addresses, telephone numbers and social media handles, with signals routed to trusted external partners to support disruption of scam infrastructure.

This illustrates the wider opportunity that an effective trusted-flagger framework could provide. An online provider may identify a particular advertisement or account, while another organisation may hold relevant intelligence concerning the URL, domain, telephone number, identity or other infrastructure associated with that activity. Bringing together intelligence from different parts of the fraud ecosystem can provide a richer basis for identifying and disrupting fraud than organisations acting on their own information in isolation.

Cifas therefore considers that collaboration should be at the core of the trusted-flagger model. Fraud prevention will be most effective where providers can draw appropriately on intelligence from across

the wider ecosystem rather than operating within organisational or sectoral silos. This is consistent with Cifas's established position that organisations holding critical data on fraud, scams and the criminals perpetrating them should form part of trusted-flagger arrangements, and that implementation of the Online Safety Act should facilitate the sharing of data and intelligence across key sectors and into online platforms.

We therefore encourage Ofcom to ensure that the framework is capable of recognising appropriate fraud-prevention bodies and organisations holding high-quality cross-sector data and intelligence as trusted flaggers, where they can demonstrate the necessary expertise and appropriate standards of governance, data quality and security. This should complement the important role played by law enforcement, regulators and other expert organisations.

A trusted-flagger framework that is drawn too narrowly risks excluding valuable sources of fraud data and intelligence simply because they sit elsewhere in the ecosystem. This could mean providers are expected to identify and act against fraudulent advertising without benefiting from relevant intelligence held by organisations that may be able to help identify that activity earlier and reduce the risk of harm.

Q23. Do you agree with Ofcom's overall proposal for ad libraries?

Cifas supports the principle of effective ad libraries where they enable users and expert organisations to identify and report suspected fraudulent advertising.

From a fraud-prevention perspective, their value extends beyond individual advertisement lookup. Ad libraries could provide a valuable source of intelligence both proactively, by helping identify current patterns and potentially linked activity, and retrospectively, by allowing previous advertisements and associated information to be examined when new fraud intelligence emerges.

Cifas therefore considers that the utility of ad libraries should be assessed not only by the information they make publicly available, but by how effectively that information can be searched, analysed and incorporated into fraud-prevention activity. We welcome Ofcom's proposal for API access, which it identifies as enabling experts to identify new and evolving fraudulent-advertising trends and undertake cross-service comparisons.

We would encourage Ofcom to go further by considering fuzzy-matching capability, enabling investigators to identify close or approximate matches rather than relying solely on exact search terms, particularly where criminals make small changes to names or other identifiers in an attempt to evade detection. This is a Cifas recommendation beyond the functionality explicitly identified in the current proposal.

Cifas would also encourage Ofcom to consider whether appropriate ad-library information could be downloadable or otherwise made available in structured, machine-readable formats, subject to proportionate privacy, security and anti-abuse safeguards. Combined with API integration, this could allow relevant advertising signals to be incorporated into wider fraud-detection and prevention processes rather than requiring experts to interrogate each library manually.

Ad libraries consequently have the potential to become more than transparency repositories. Properly designed, they could provide actionable fraud signals that support pattern identification, cross-platform analysis and both proactive and retrospective prevention activity.

We therefore support Ofcom's proposal and recommend that the final requirements place particular emphasis on searchability, historical visibility, API integration, appropriate downloadable or machine-readable access, and the potential for fuzzy matching, while maintaining appropriate privacy and security safeguards.

Q24. Do you agree with the proposed ad-library principles, functionality and information categories?

Cifas broadly supports Ofcom's proposed approach, particularly effective searchability, historical visibility and structured access that can help identify repeat or linked activity.

We recommend that Ofcom test the final information requirements with organisations that will use ad libraries for fraud detection and investigation. The objective should be operational utility and actionable intelligence rather than publication of data for its own sake.

Information requirements should also be assessed against the risk that excessive transparency could expose detection methods or personal information.

Q25. What evidence can you provide on the resources and time required to build or adapt an ad library?

Cifas does not currently hold sufficiently robust evidence on the engineering resources, cost or implementation time required for a service provider to build an ad library from scratch or adapt an existing library to Ofcom's proposed specification.

We therefore do not offer an implementation estimate. Providers operating these systems and specialist technical organisations are better placed to provide that evidence.

Cifas can contribute a fraud-prevention perspective on the functionality that makes advertising information useful for identifying and reporting suspected fraud, including searchability, historical visibility and the ability to identify patterns or linked activity.

Conclusion

Cifas welcomes Ofcom's proposed Fraudulent Advertising Codes and supports their prevention-first, layered approach. The final Codes should ensure that responsibility does not begin only once a consumer reports a suspicious advertisement. Effective prevention requires strong account integrity, continuously evolving fraud-risk assessment, proportionate moderation and effective use of intelligence from outside individual platforms.

Central to this should be a broad, diverse and responsible trusted-flagger ecosystem. No single organisation holds a complete picture of fraud risk. Valuable intelligence sits across financial services, technology, telecommunications, law enforcement, regulators and specialist fraud-prevention organisations. The effectiveness of the Codes will therefore depend, in part, on ensuring that this wider intelligence can reach the platforms capable of acting upon it.

The Fraudulent Advertising Codes provide an important opportunity to embed that collaborative approach into the UK's response to online fraud. Cifas stands ready to work with Ofcom, service providers and other partners to support effective implementation, including the development of a

sufficiently broad and effective trusted-flagger network and the responsible use of cross-sector fraud data and intelligence.