Consultation response

Field	Value
Responder	The Investment Association
Responder Type	organisation
Org Role	Senior Policy Analyst - Financial Crime
Org Type	Other
Other Type	Trade Association for the Investment sector

Volume 1: Context

3. Online advertising ecosystem

Q1: Is there any information or evidence you hold that could enhance our understanding of the online advertising ecosystem?

The IA's members do not provide online platforms, search engines or advertising systems. However, they and their customers are affected by fraud perpetrated by criminals who exploit those systems to promote fraudulent schemes, frequently by impersonating legitimate investment firms. One recent fraud methodology, originating from social media adverts on Facebook and Telegram in which criminals impersonated the brands of UK investment firms, led to thousands of individuals losing significant sums. Members have also recently reported brand-cloning frauds appearing on platforms they had not previously seen used for this purpose, including TikTok. This illustrates how quickly fraudsters adapt to new channels.

4. Causes and impacts of fraudulent advertising

Q2: Do you have any comments on Ofcom's assessment of the causes and impacts of fraudulent advertising? Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.

Fraudulent investment adverts, clone-firm promotions and the impersonation of legitimate investment managers expose consumers to serious financial harm, undermine confidence in regulated financial services and impose substantial costs on firms whose identities and brands are misused. Anecdotal evidence from members indicates that the majority of investment frauds identified by investment firms originate with some form of online advertising. Report Fraud's latest Annual Assessment notes that it has "become the norm for fraudulent investment opportunities to be promoted via social media and direct messaging platforms" (https://www.reportfraud.police.uk/uploads/The_Report_Fraud_Annual_Assessment_FY_2025_26_Cyber_Crime_and_Fraud_Official_1_8fc22fd941.pdf).

The impact on impersonated firms deserves particular weight. By the time an investment firm becomes aware that its brand has been impersonated, the advert will already have been accepted, targeted and distributed, and numerous consumers may already have been exposed to harm. The firm must then investigate the incident, warn consumers and seek the removal of content from systems over which it has no control.

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

The IA does not comment on the individual examples. From the experience of investment firms, the characteristics of particular concern are: the impersonation of regulated firms, including by clone firms using genuine regulatory details without authority; advertisers on the FCA Warning List; the takeover of legitimate accounts; banned advertisers returning through new identities, intermediaries or compromised accounts; and the rapid displacement of fraud to new platforms. We comment on these further under Volume 3.

5. Our approach to developing Codes measures

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

Yes. The IA supports Ofcom's emphasis on safety by design, advertiser verification, account integrity, fraud indicator assessments and effective moderation. The proposed layered approach appropriately prioritises preventing fraudsters from accessing advertising systems, while improving detection and ensuring the swift removal of content that evades initial controls. These measures, particularly financial services verification, account banning and ad libraries, reinforce one another and would be significantly less effective if treated as standalone proposals. Ofcom should retain them in the final Codes and should not dilute them in a way that weakens platforms' responsibility to prevent consumer harm before it occurs.

Fraudsters are adaptive and adept at exploiting any weakness, ambiguity or 'grey area' in the design of rules and controls. As controls on one service are strengthened, criminal activity is quickly displaced to another. Ofcom should therefore keep the Codes under periodic review so that they keep pace with fraudsters' evolving methods.

The credibility of the framework will depend on effective supervision and enforcement. Ofcom should actively test whether providers are delivering the required safety outcomes in practice and take timely, proportionate and dissuasive action where they fail to meet their legal duties. Without credible oversight and meaningful consequences for non-compliance, even the strongest Codes risk having limited practical effect. Success will also depend on Government providing Ofcom with the necessary political support, resources and powers.

6. Combined impact assessment

Q5: Do you consider the overall burden on the service providers in scope of our proposed measures to be proportionate? Please provide any arguments and supporting evidence.

Yes. Primary responsibility for identifying and preventing fraudulent advertising should rest with the platforms, search services and relevant intermediaries that are paid to host, place or distribute such advertising. These businesses control the advertising environment, determine who may access it and derive revenue from it, so they are best placed to prevent their services from being exploited.

This reflects, by analogy, the "polluter pays" principle. The costs of preventing and addressing harm should principally be borne by those whose services enable the activity, who benefit financially and who are best placed to control the risks. They should not be transferred to victims or to legitimate organisations affected by the fraud. This does not make platforms responsible for the underlying criminal intent. It does mean that businesses operating and monetising advertising systems should bear primary responsibility for protecting those systems from abuse. Investment firms should not, in effect, be expected to monitor advertising systems on behalf of the businesses that operate and profit from them.

Volume 2: Risk, governance and control

2. Advertising intermediaries

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

Yes. The use of advertising intermediaries or open-display supply chains should not dilute providers' responsibility. Providers should remain accountable for the safety outcomes experienced by users and should impose appropriate requirements on intermediaries performing relevant advertising functions. A provider's choice of advertising pathway should not fragment accountability or result in weaker protections.

Q7: We have included two illustrative examples of when and how this measure may be applied, and what 'all reasonable endeavours' might look like. Do you have any comments on these examples, and do you have any additional examples of how providers could work with or require intermediaries to implement safety measures in circumstances where they have insufficient control? Please provide any arguments and supporting evidence.

No response

3. Fraud indicator assessment

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

Yes, but it should go further. Ofcom refers to information sharing in the fraud indicator assessment proposal, but this does not appear to impose a proactive obligation to share fraud signals. Ofcom should require categorised services to share relevant fraud signals with one another. Identification of a fraudulent advertiser or account should trigger the sharing of signals, such as email addresses, phone numbers, linked accounts or other account-level signals, with other categorised services. This would help stop fraudsters moving across platforms and reappearing elsewhere.

Q9: Do you think there are other information sources providers should consider in order to understand how fraudulent advertising manifests on their service? If so, what information and why would they need to consider it?

Providers should draw on intelligence from trusted flaggers, regulators (including the FCA Financial Services Register and Warning List), law enforcement and impersonated firms. These sources can provide valuable intelligence, particularly where new fraud methods have evaded preventative controls. Providers should also use fraud signals shared by other categorised services, and the results of testing their controls against known and emerging fraud methodologies.

4. Governance and accountability

Q10: Do you agree with our proposals? Please confirm which proposed measure your views relate to and provide any arguments and supporting evidence.

Yes. Governance arrangements should include regular, risk-based review and testing of the processes underpinning the Codes, to make sure they are not being gamed or circumvented by fraudsters. These reviews should draw on fraud indicator assessments and on intelligence from trusted flaggers, regulators and law enforcement. Providers should be able to evidence to Ofcom the outcome of each review and any changes made as a result. Ofcom should also set clear expectations on how intelligence from experts is built into systems, controls and operational decision-making, and on how providers demonstrate this to both Ofcom and the experts concerned.

5. Testing advertisement generation tools

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

No response

Volume 3: Ensuring account integrity

2. Account checks and actions

Q12: Do you agree with our proposal? Please provide any arguments and supporting evidence. Where your feedback relates to a specific check we are proposing providers should carry out, please make this clear. These are :

Yes. Ofcom's proposed account checks and restrictions on fraudulent advertisers are important. Action should extend beyond removing an individual advert: providers should investigate linked accounts and other relevant indicators, restrict repeat offenders and prevent banned actors returning through new or existing accounts.

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

Advertiser verification needs to be robust. A fraudster who succeeds in passing verification acquires a veneer of legitimacy that would undermine trust in the system as a whole.

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

Fraudsters will seek to evade these measures through new identities, intermediaries or compromised accounts, so the controls should be regularly reviewed and tested.

Q12.C: checks for accounts with indicators that there is a material risk they will post fraudulent advertising so that restrictions can be applied to them

See our comments on linked UGC accounts under Advertising bans.

Q12.D: repeat checks where there are relevant changes identified on an account.

No response

Q13: Are you aware of any other account checks and actions providers could do to protect users from fraudulent advertising? Please provide any arguments and supporting evidence.

Identifying a fraudulent advertiser should trigger the sharing of fraud signals with other categorised services (see our response on the fraud indicator assessment). It should also lead to linked user-generated content (UGC) accounts being treated as high risk (see Advertising bans).

3. Preventing fraudulent financial services advertising

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

The IA strongly supports Ofcom's proposal that providers should apply a financial services verification policy which, as a minimum, checks FCA authorisation using the FCA Financial Services Register and checks against the FCA Warning List. Wherever technically practicable, these checks should be built into providers' advertiser onboarding and ongoing monitoring processes, not applied only after an advert has been reported. Verification should be risk-based and completed before financial services adverts are published. Providers should also compare the advertiser's identity and associated details with the relevant regulatory record, and remain alert to clone firms using genuine regulatory information without authority.

If categorised services choose to accept paid-for financial services advertising, it is proportionate to require them to develop sufficient understanding, systems and controls to identify clear breaches of the financial promotions regime and other relevant FSMA offences captured by the Online Safety Act.

4. Countering account takeover

Q15: Do you agree with our proposals? Please confirm which proposed measure your views relate to and provide any arguments and supporting evidence.

Yes. Financial services verification may be defeated by the takeover of legitimate accounts, as well as by clone firms. Banned advertisers may also seek to return through compromised accounts. Controls in this area should be regularly reviewed and tested.

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

No response

5. Advertising bans

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

Yes. The banning of accounts is core to preventing repeat offenders and is among the most important measures to reduce fraud. In April 2026 the FCA found that 66% of the illegal financial advertisements it identified on social media platforms were linked to firms or individuals already on its Warning List (https://www.fca.org.uk/news/press-releases/fca-spearheads-global-action-stop-illegal-finfluencers). This underlines the value of both Warning List checks at onboarding and robust controls against repeat offenders.

However, banning a fraudulent advertiser will have limited effect if their related UGC accounts continue to operate unchecked. A ban for fraudulent advertising should result in linked UGC accounts being treated as high risk. Those accounts should then be subject to further review, content moderation judgements or other proportionate risk-based action, such as removing their content from recommender systems.

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

The IA does not propose additional circumstances. Any route to reversing bans should be tightly controlled, because fraudsters may seek to exploit it to reinstate banned accounts.

6. Account appeals

Q19: Do you agree with our proposals? Please confirm which proposed measure your views relate to and provide any arguments and supporting evidence.

Account appeals and advertising complaints processes could be exploited to reinstate banned accounts or otherwise frustrate enforcement action. Providers should regularly review and test these processes to make sure they are not being gamed by fraudsters.

Volume 4: Moderation

2. Advertising moderation

Q20: Do you agree with our proposals? Please confirm which proposed measure your views relate to and provide any arguments and supporting evidence.

Yes. The final framework should support proactive detection and appropriately resourced moderation, so that fraudulent content that evades preventative controls is swiftly identified and removed. The overriding objective should be to interrupt fraud early in the customer journey, before consumers are exposed and funds are transferred.

3. Terms of service and publicly available statements

Q21: Do you agree with our proposals? Please confirm which proposed measure your views relate to and provide any arguments and supporting evidence.

No response

4. Advertising complaints (including DRC for trusted flaggers)

Q22: Do you agree with our proposals? Please confirm which proposed measure your views relate to and provide any arguments and supporting evidence.

Reporting should be a secondary safeguard, not the principal means of identifying fraudulent advertising. The regime should not depend on victims or legitimate firms continuously monitoring platforms and reporting individual adverts after publication. Even so, accessible reporting channels and trusted-flagger arrangements remain important.

At present, the design of reporting channels is left to each provider, and in practice these interfaces can make it difficult to submit, manage and track reports. Ofcom should require user-friendly reporting tools, including functionality that lets trusted flaggers monitor the status, history and outcomes of their reports. Providers should also give proactive feedback that shows, as a minimum, whether a report is under review, whether the review has been completed and what action, if any, has been taken.

5. Ad libraries

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

Yes. The IA supports improved transparency through ad libraries, which form part of a mutually reinforcing set of measures. However, ad libraries could also be used by fraudsters to identify which fraudulent adverts have successfully evaded detection. Providers should keep this risk under review.

Q24: Do you agree with the principles, functionalities and information categories which we have included in the proposed measure? Please explain your reasoning and, if possible, provide supporting evidence.

No response

Q25: Do you have any evidence or insights on the process of building an ad library from scratch or adjusting an ad library to align with the proposed measure, and how long that process would take?

No response

Additional questions

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

No response

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

No response

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

Providers accepting financial services advertising should be able to identify clear breaches of the financial promotions regime and other relevant FSMA offences captured by the Online Safety Act.