FCA Response to Ofcom's Fraudulent Advertising Codes Consultation

I. Executive Summary

1. Fraud reached a four-year high in 2025. It has severe financial and emotional impacts on victims, with investment fraud accounting for the largest losses (£221.5 million) and increasing by 40% year-on-year (UK Finance, 2026)[1]. Social media is the most common place where consumers encounter online scams, cited by 65% of UK adults. Around half (51%) of UK adults report frequently seeing adverts they suspect are scams, while one in four say they have lost money after clicking on a fraudulent advert (Public First, 2026)[2]. This not only causes direct consumer harm but also undermines confidence in financial markets, with concerns about scams cited as the main reason many UK consumers hesitate to invest (capital.com)[3].
2. We welcome the proposals for categorised services announced in the Consultation. Robust measures against fraudulent advertising, especially on services of such high reach and impact, are of critical importance for strengthening consumer protection. The proposed Codes provide an ambitious starting point to materially improve consumer protection if implemented, supervised and enforced effectively.
3. We consider that the following core measures are particularly important to stop fraud in the advertising ecosystem:
    a. **Financial Services verification**, including checks against the FCA Register and FCA Warning List;
    b. **Advertising bans**, including measures for account checks to prevent repeat offenders returning;
    c. **Ad Libraries**, including robust search functionality, API access, targeting information and advertiser identity information.

[1] Annual Fraud Report 2026, UK Finance
[2] Public First, 2025 [*Clicking with caution – How scams adverts are damaging the online economy*], commissioned by Revolut.
[3] Capital.com, 2025, [*Fear or fortune? A research report assessing attitudes to investment and risk in the UK]*

4. In the pages below, we draw on evidence from our work to support the proposed measures and their objectives. We also identify opportunities to strengthen the Codes further, particularly:
    - Enhancing the effectiveness of accounts bans through **cross-platform intelligence sharing** and expanding linked account checks to include **User Generated Content (UGC) accounts.**
    - Strengthen **outcome focused requirements** particularly for Governance and Moderation measures.
    - Targeted enhancements to improve the operational effectiveness of the **Dedicated Reporting Channel** and **ad library** proposals.
    - Better aligning the **Illegal Content Judgement Guidance** with the expectations set under the Financial Services verification measure.
5. We would welcome Ofcom using its Transparency Reporting powers to make platforms publish comparable metrics to evidence the impact of these measures.
6. We'll continue to work with Ofcom, including on its upcoming proposals for proactive monitoring, in the development and implementation of the final proposals.
7. Annex 1 contains a reference list of our summarised recommendations for enhancements of the Fraudulent Advertising Codes.

II. Detailed response by Volume

Volume 2: Risk, governance and control

8. We support Ofcom's proposed Risk, Governance and Control measures. Similar accountability and governance requirements have been instrumental in embedding a cultural change and strengthening firms' approach to fraud prevention in financial services. For example, the Senior Managers and Certification Regime (SM&CR) in the UK is a well-established regulatory practice requiring firms to allocate clear individual responsibilities to senior managers, supported by statements of responsibility setting out what they are accountable for. Respondents to an FCA Discussion Paper[4] overwhelmingly supported the view that SMC&CR has made it easier to hold individuals to account and that it supported conduct within firms.

9. FCA reviews of firms processes and controls[5] identified examples of good and poor practice that may be relevant for Ofcom in considering these measures and how to supervise them in practice. For example, poor practice involved firms' senior management not challenging business wide risk assessments.

10. The success of the measures will ultimately depend on whether they deliver meaningful outcomes, rather than being treated as a 'tick box' exercise of having documented policies, processes and responsibilities.

Measure FAU B1: Fraud Indicator Assessment

11. We suggest that the code should explicitly set out that providers should proactively seek external expertise and intelligence to inform their fraud indicator assessment. Fraudsters constantly adapt their methods in response to detection and enforcement measures. Requiring platforms to engage regularly with external experts, including regulators, law enforcement, consumer organisations and specialist fraud bodies, would help ensure that assessments remain informed by the latest intelligence and reflect the changing nature of fraud risks.

12. Service providers should be required to demonstrate what action they have taken in response to the expert views they receive. For example,

[4] See paras 3.2 – 3.8 of CP 25/21 https://www.fca.org.uk/publication/consultation/cp25-21.pdf
[5] https://www.fca.org.uk/publications/good-and-poor-practice/risk-assessment-processes-and-controls-firms-our-findings

provide an annual report to their most senior governance body setting out the intelligence received from experts and what action was taken in response to this intelligence. This would encourage meaningful engagement rather than a purely procedural consultation exercise. Where expert recommendations are not adopted, platforms should explain their rationale. Such a requirement would help ensure that Fraud Indicator Assessments remain effective over time.

13. This would address a major challenge the FCA currently faces in its engagement with tech companies. Intelligence the FCA shares, including on fraud typologies, fraudsters methods and emerging illegal content trends, has not consistently translated into meaningful improvements in fraud prevention.

14. We would welcome Ofcom using its Transparency Reporting powers to compliment this measure. Requiring platforms to publish clear metrics on rates of fraudulent advertising on their platform, and the impact of their measures on volumes of fraudulent advertising, will help drive clear accountability and a focus on end outcomes. We consider that any metrics should be: i) comparable across platforms; ii) outcomes-focused; and iii) use a combination of relative numbers (proportions, rates, etc.) and absolute figures. Please see the FCA's response to Ofcom's Transparency Reporting consultation for further details.

Measure FAU F1: Testing Advertisement Generation Tools

15. We support this measure. We recommend that the code measure should expressly require providers to take appropriate steps to mitigate risks identified in the testing. Whist the chapter expects providers to do this, it is not reflected as an explicit requirement in the Code measure itself.

16. Reuters'[6] reporting from December 2025 illustrates why this measure is essential, highlighting the risk that Meta's advertising tools may assist in placing fraudulent investment ads, and that its own AI tools may suggest ways to amplify such content by improving it. This reinforces the need for providers to test whether AI and advertising

[6] https://www.reuters.com/investigations/metas-trusted-experts-helped-me-run-scam-ads-facebook-instagram-2025-12-15/

tools can facilitate the creation, optimisation or scaling of fraudulent advertising.

Volume 3: Ensuring Account Integrity

17. We strongly support Ofcom's account integrity measures. We also support the expectations on providers to repeat checks when circumstances change and to regularly review their policies. To maximise impact and ensure consistency across the Codes, providers should also be expected to consider expert intelligence and feedback when reviewing and improving these measures, as proposed for ad libraries. Below, we set out our views on specific measures and opportunities to strengthen them further.

Measure FAU H1: Account checks and actions

18. In our experience, fraudsters often return using new identities or migrate slightly altered content to another account. Effective account checks are, therefore, critical to the success of the advertising bans measure. Customer Due Diligence (CDD) and onboarding checks such as Know Your Customer (KYC) requirements are a fundamental practice in the payments and banking sectors as a key friction and control against fraud. Applying similar expectations to tech companies and their systems would help tackle similar harms from fraud enabled by tech platforms. We also welcome the requirement for providers to document their account-check policies.

19. A limitation of the proposals is a lack of cross-platform information sharing. Ofcom should consider requiring categorised services to share proportionate fraud signals linked to identified fraudulent accounts, such as email addresses, phone numbers and other accounts signals. Fraudsters routinely reuse these identifiers across multiple services, so sharing them would help platforms identify connected accounts, prevent fraudulent advertisements, and enable faster, more effective takedown of related activity. This would ensure providers use relevant intelligence to protect users on their own services. This is not about making one provider responsible for activity elsewhere. It is about ensuring that each provider uses relevant intelligence to prevent fraudulent advertising on its own service.

20. Information sharing would also enable faster and more complete takedown. When one fraudulent account is detected, the associated signals could help other platforms locate and remove connected advertisements and accounts before further harm occurs. Without this requirement, each platform must rediscover the same fraud

independently, allowing criminals to move between services and continue targeting consumers while individual advertisements are removed in isolation. Ecosystem-wide information sharing is therefore a necessary input to effective prevention and takedown on each service

21. The ICO has made clear[7] that UK data protection law does not prevent appropriate information sharing to prevent harm. The main barriers to information sharing are a lack of incentives and regulatory requirements, rather than legal constraints.

22. There is significant evidence from other sectors that intelligence-sharing materially improves financial crime outcomes. For example, Data Fusion[8], a public-private initiative led by the National Crime Agency (NCA) and the National Economic Crime Centre (NECC), combines targeted transaction data from seven UK banks with NCA crime-related datasets, analysed by a joint team of NCA and bank experts. Its outputs inform the NCA's investigative work and help the banks identify risk. Between May and June 2024, it delivered 90 intelligence packages, supported high-priority investigations into organised immigration crime, fraud and money laundering, identified eight organised crime networks, and shared intelligence back with banks to improve their defences.

23. This would complement and support ongoing efforts to support stronger intelligence sharing from the tech sector. Service providers could meet this obligation through supporting existing initiatives such as Stop Scams UK, the Online Crime Centre and Global Signals Exchange. A regulatory expectation is critical to support these efforts, as currently platforms are not doing enough to share information about known fraudulent accounts.

24. If Ofcom does not consider that it can require providers to disclose fraud signals proactively to other services, it should expect providers, as part of their Fraud Indicator Assessment, to seek relevant intelligence from other categorised services about fraudulent advertisers and accounts. Expecting each provider to seek this intelligence would help it identify whether actors already detected elsewhere are using, or attempting to use, its own service. This would strengthen the assessment by ensuring it reflects known fraud

[7] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/sharing-personal-information-when-preventing-detecting-and-investigating-scams-and-frauds/
[8] Ground breaking public private partnership launched to identify criminality using banking data - National Crime Agency

patterns beyond the provider's own data and supports earlier intervention against fraudulent advertising.

25. We consider that this approach would build directly on Ofcom's existing proposal. The purpose of requesting the information would be to improve prevention on the requesting provider's own service, allowing it to check for connected accounts, strengthen its detection systems and stop fraudulent advertisements before consumers encounter them. It would also help minimise the length of time any fraudulent content is present on the platform, by ensuring that the platform can effectively look for known fraudsters and identify and take down their content.

Measure FAU H2: Preventing fraudulent financial services advertising

26. We strongly support this measure. It complements requirements under financial services law. This measure is proportionate and technically feasible to implement, as several categorised services claim to have already implemented financial services advertiser verification following engagement with the FCA[9].

27. We have seen clear improvements where services have voluntarily restricted financial advertising to FCA-authorised firms. For example, this led to a ~100% reduction in scam ads on Google when first adopted financial service verification policies. Bringing these existing voluntary arrangements into a regulatory requirement would strengthen incentives for consistent implementation and enable Ofcom to take enforcement action where platforms fail to apply these checks effectively.

28. We particularly welcome the proposed requirement to check advertisers against the FCA Register and Warning List. During our international week of action in April 2026, 66% of the financial adverts we reported were linked to persons already on the Warning List (FCA). Verification checks against the Warning List could have prevented those ads from reaching consumers in the first place.

29. Financial Services verification should not be treated as a one-off control. We recommend that, similarly to the ad libraries measure, providers be expected to regularly engage with experts and take into

[9] This includes Google, Bing, Facebook, Instagram, X and TikTok

account recommendations for enhancements to their financial services verification processes. This would help ensure the measure remains effective as fraud tactics evolve.

30. This also supports the need for forthcoming consultation on proactive technologies. Proactive detection of financial services advertising will be critical to the success of FAU H2. In our experience, one of the main weaknesses in platforms' financial services verification systems is whether they correctly identify, at the outset, that the advert relates to financial services and should therefore be subject to enhanced verification. If this initial detection stage is ineffective, fraudulent financial promotions may avoid the verification process entirely. Platforms already claim to use a range of proactive detection methods to identify financial services ads. We therefore consider that a financial services proactive technology measure would be proportionate and technically feasible.

Measure H5: Advertising bans

31. We strongly support this measure. Most of the fraudulent content we identify through our 'weeks of action' are linked to persons the FCA has previously reported to social media platforms. This measure has the potential to significantly reduce phoenixing and life boating practices by fraudsters. To strengthen this measure we recommend stronger expectations around linked User Generated Content (UGC) accounts that fraudsters could still use to post fraudulent content.

32. We consider that a finding of fraudulent advertising should, as a minimum, trigger heightened scrutiny of associated UGC accounts and appropriate risk-based action to reduce potential ongoing harm. This may include undertaking a content moderation assessment on the account and removing content from recommender systems. We understand that this may require a new measure under the Illegal Content Codes.

Volume 4: Moderation

Measure FAU E1: Ad libraries

33. We strongly support Ofcom's proposals. Effective ad libraries are fundamental for supporting trusted flaggers and other organisations with identifying and reporting illegal content and assessing the effectiveness of platforms controls for preventing fraudulent content. We believe these measures are proportionate and technically feasible given equivalent requirements in the EU the platforms must comply with. We particularly support the following parts of the proposal:

    a. The suite of information that providers should be ready to set out, and to be 'reliable' and 'consistent'.

    b. The expectation that ad libraries are updated daily and keep an evidential record for at least 12 months after they were last live.

    c. The ask on providers to regularly consult with experts and consider their recommendations to improve and update their ad libraries. As noted above, we also consider this a desirable addition to the part of the Accounts Checks measure (FAU H1) and Financial Services Verification measure (FAU H2).

34. It is important that ad libraries are publicly accessible, rather than being limited only to trusted flaggers or a closed group of nominated organisations. This materially strengthens the effectiveness of the fraudulent advertising regime by enabling a wider network of actors, including journalists, researchers, consumer groups, impersonated brands and members of the public, to identify and report fraudulent advertisements. This is particularly important for detecting fraudulent brand impersonation and deepfake advertising, where the individuals or organisations being impersonated are often best placed to recognise misuse of their name, image or reputation. Recent reporting by the *Financial Times*[10] demonstrates this: public access to ad libraries enabled Martin Wolf to identify deepfake advertisements impersonating him, bring them to public attention and highlight weaknesses with Meta's systems for preventing fraudulent advertising.

35. Public ad libraries also support scrutiny that creates incentives for platforms to improve their prevention and moderation systems. Public ad libraries increase the likelihood that fraudulent advertisements are identified, reported and removed; improve the detection of emerging

[10] https://www.ft.com/content/80d9c4f8-653d-4f8c-89b8-b4d1e183a134?syn-25a6b1a6=1

fraud typologies; and supports independent scrutiny of whether platforms are effectively meeting their obligations. Restricting access to a closed group of organisations would significantly reduce these wider preventative and accountability benefits and weaken the effectiveness of the regime as a whole.

36. We recommended targeted changes to improve the operational effectiveness of this measure including:

a) **Include 'actual reach' as a mandatory field:** Target reach shows only the audience an advertiser intended to reach. It does not show how many users were actually exposed to the fraudulent advertisement. Actual reach is therefore necessary to measure the scale of consumer exposure, identify the advertisements causing the greatest harm and assess whether providers' systems and processes are delivering effective outcomes. Without actual reach information it will be harder for experts to assess whether service providers are effectively preventing individuals from encountering fraudulent advertisements and minimising the time those advertisements remain present. We are also concerned that fraudsters would attempt to 'game' target reach data to avoid detection.

b) **Time period the ad was live (start and end date)**: This will enable law enforcement and consumers who encounter a suspected fraudulent advertisement to search the relevant period, locate the advert and report it for removal. Requiring this information directly supports the duties to minimise the time fraudulent advertisements remain present and to take them down swiftly once a provider is alerted to them. Without a searchable record of when an advert ran, it may be difficult to identify the relevant content and report it for action. Several platforms already provide this data, so we consider it proportionate to include.

c) **Identity of the person responsible for placing the ad and paying for the ad**: the code should require providers to identify both: i) the legal entity/natural person placing and responsible for the ad; and ii) the legal entity/natural person who paid for the ad. These may not always be the same person. Advertisers' names alone may be unclear particularly where advertising is placed by intermediary agencies on behalf of clients. This information would help connect advertisements placed through different accounts, identify wider networks of fraudsters and enable action against

related advertisers and content. This information is also important to support more effective prevention and takedown by allowing providers, regulators and law enforcement to disrupt the actors behind a fraudulent campaign, rather than removing individual advertisements only for the same fraudsters to reappear through different accounts.

d) **Change code description**: from *'ad library should contain the following information'* to *'ad library should contain, as a minimum, the following information'*. This would prevent providers from arguing that the Codes create a ceiling on what can be included in the ad library and would more closely align with Ofcom's policy intention in the body of the consultation, which describes the proposed information requirements as a minimum (p.5.9).

Measure FAU D1-D7: Dedicated Reporting Channels (DRC)

37. The FCA welcomes being included as a trusted flagger and supports the addition of other relevant partners. We would also support including the Cyber Defence Alliance as a trusted flagger given their valuable expertise and resources allocated to finding and reporting fraudulent advertising.

38. We remain concerned that the DRC measure is too reactive and similar to the measure introduced in the Illegal Harms Codes. In our experience, the DRC measure has not worked as we had hoped. Reporting interfaces vary significantly across services and are not always configured to support efficient reporting. Some require highly manual and time-consuming steps, particularly where connected illegal content appears across multiple services, accounts or formats. This creates unnecessary operational burden for trusted flaggers, materially undermining the effectiveness of this measure in practice.

39. We recommend enhancing the DRC measure by including expectations that reporting channels should be user friendly, easily accessible and capable of supporting efficient reporting of connected illegal content at scale. This should include making it easy for trusted flaggers to track previous reports and the action taken in response to these reports.

40. Service providers also do not provide transparency on their decision making. In particular whether they are taking action over a breach of their community standards or 'only' a local law breach. We

recommend that service providers should be required to provide transparent moderation decisions to trusted flaggers in response to their reports.

41. These issues will not improve while the measure does not set minimum expectations on ensuring DRC's are effective in practice. If this measure is left unchanged, we are concerned that providers could comply just by having a dedicated reporting channel, even if in practice it is not effective and does not assist trusted flaggers.

Measure FAU C2: Advertising Moderation

42. We support the moderation measures in the consultation. However, we recommend providing clearer expectations on how they should work in practice. While we appreciate some judgements on complex cases could take longer, we consider that the Code should define timelines for "swiftly" taking down fraudulent advertising once providers become aware of it (through reporting and detection), including a baseline expectation that fraudulent ads reported by trusted flaggers should be reviewed and actioned immediately, and no later than 24 hours after reporting.

43. There continues to be significant variation in how quickly platforms respond to FCA reports of illegal content; from less than an hour to several weeks. The proposed US settlement with Meta[11] would require it to respond within six hours to 90% of the reports from teenagers concerning harmful content. The UK Government has been clear in its expectations to extend protections agreed in the US to the UK, so that UK users should not receive a lower level of protection.

[11] Attorney General Bonta Secures Transformative $17 Billion Settlement with Meta.

Fraudulent Advertising - Illegal Content Judgement Guidance

44. We are concerned by the position set out in the Illegal Content Judgement Guidance, which appears to suggest that providers should not be expected to develop detailed expertise in FSMA offences. This risks creating uncertainty and undermining the effectiveness of the financial services verification measure. It is also inconsistent with the FCA's expectations of providers and financial services law.

45. In the context of paid-for advertising, the assessment is significantly simplified. A paid-for advertisement will inherently be promotional and made in the course of business. The main assessment a provider will need to make is whether the ad relates to financial services. It is entirely reasonable and proportionate for service providers to make this type of assessment, particularly given these will be categorised services with significant resources and existing advertising policies.

46. Where platforms choose to carry paid-for financial services advertising, it is proportionate to expect them to develop sufficient understanding, systems and controls to identify clear breaches of the financial promotions regime and other relevant FSMA offences. The FA ICJG should therefore align closely with the financial services verification measure and avoid implying that such judgements are beyond providers' capabilities, as this could weaken both the verification measure and the proposed proactive detection requirements. We are happy to work with Ofcom on alternative wording.

Annex 1: Summary of recommendations for enhancements

Measure	FCA Recommendation
Volume 2: Risk, Governance & Control	
FAU B1: Fraud Indicator Assessment	Service providers should proactively seek and use external expert intelligence, including from trusted flaggers, to inform fraud indicator assessments.
	Service providers should demonstrate what action they have taken in response to intelligence providers by external experts.
	Ofcom should require platforms to publish outcome focused metrics on fraudulent advertising using its Transparency Reporting powers.
FAU F1: Testing Ad Generation tools	The Code should expressly expect providers to mitigate any risks identified through the testing of advertisement generation tools.
Volume 3: Ensuring Account Integrity	
FAU H1: Additional account checks	Introduce ecosystem-wide expectations for providers to share fraud signals linked to identified fraudulent accounts with other categorised services.
FAU H2: Preventing fraudulent financial services advertising	Providers should regularly engage with experts on their approach to financial services verification and take into account their recommendations for improvements.
FAU H5: Advertising bans	A finding of fraudulent advertising should trigger additional checks on linked UGC accounts. For example, performing content moderation assessments on UGC accounts and removing content from recommender systems.
Volume 4: Moderation	
FAU C2: Advertising moderation	The Code should define a minimum expectation for what constitutes "swiftly" takedown of fraudulent advertising once providers become aware of it, including a baseline expectation that fraudulent ads reported by trusted flaggers should be reviewed and actioned immediately, and no later than 24 hours after reporting.
FAU D1-D7: DRCs	Include the Cyber Defence Alliance (CDA) as a trusted flagger.
	The Code should set minimum expectations for DRCs, including efficient reporting interfaces, transparency on decision making, and use of trusted-flagger intelligence to improve proactive moderation.
FAU E1: Ad Libraries	Expand the information requirements to include: - actual reach, alongside target reach; - the time period the add was live (start date and end date); - Include details on the person responsible for placing the ad (legal entity or natural person). - payee information to identify the person/entity paying for the ad, including where this differs from the advertiser;
	Amend the code to state that ad libraries must contain the listed information 'as a minimum'.
Illegal Content Judgement Guidance	
FA ICJG	The Fraudulent Advertising ICJG should align closely with the financial services verification measure and avoid implying that judgements are beyond providers' capabilities.