MoneySavingExpert response to Ofcom consultation

Fraudulent Advertising Codes, October 2026

Volume 1: Context

Online advertising ecosystem

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

MoneySavingExpert (MSE) supports Ofcom's assessment of the online advertising ecosystem. We agree that in both owned-and-operated and open-display supply chains, platforms play a significant role in the placement of ads on their services – whether actively or as part of their arrangements with intermediaries. The epidemic of online scams is evidence that platforms are not choosing to act responsibly within the ecosystem to ensure their users are kept safe from fraudulent advertising.

As we have set out in our campaigning many times before, we echo Ofcom's conclusion that there are very few incentives within the online advertising landscape as it currently operates to drive good safety outcomes for consumers. The lack of effective checks and balances in the current, industry-led, self-regulatory regime has created an almost Wild West situation: criminals act with no consequence; platforms profit from publishing these scams online; and countless people are scammed out of their hard-earned money every single day.

Therefore, the duties within the Online Safety Act (OSA), and by extension these proposed Codes, are absolutely crucial in improving the safety of the online space for UK consumers.

In addition, we urge Ofcom to continue its research work on the online advertising landscape, to inform the Government on the importance of further regulation of services outside the scope of the OSA. MSE remains significantly concerned about the proliferation of fraudulent advertising on news sites and, increasingly, app-based games. Urgent action must be taken to improve consumer safety across the whole online advertising ecosystem, as, once more friction is added to the process of the largest platforms, scammers will simply move on to the next easiest option.

Causes and impacts of fraudulent advertising

2. **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.**

We agree with Ofcom's assessment of the causes and impacts of fraudulent advertising. Our knowledge and strongest evidence relate to scam adverts purporting to

be of MSE's founder and executive chair, Martin Lewis, and of the MoneySavingExpert brand more generally. These ads use Martin and MSE's trusted name and reputation to trick consumers into parting with their money, often under the guise of a 'secret' investment scheme that promises incredible returns.

A typical Martin Lewis scam has the following steps:

1. A consumer comes across an ad on a social media platform, which they believe to be legitimate. It features Martin's likeness, usually alongside another public figure, and uses click-bait language designed to make the user click on it (examples of these fraudulent ads can be seen in the response to q. 3).
2. After clicking, the user is re-directed to another site, often designed to look like a BBC or other well-known media site's article. The article features fake 'quotes' from Martin and others to hook-in the user with a lucrative investment 'opportunity' which is only available for a short-time.
3. The user interacts with the article in some way, usually by inputting their personal details into a form that is sent to the scamming network.
4. The scam then moves offline, with the scammer contacting the user directly either by phone, email or WhatsApp.
5. At this stage, the activity is hard to intercept, but we have unfortunately heard so many devasting reports from our users of how the scam then progresses. The scammer uses manipulative techniques to convince the user to send them money – often this begins with small amounts which seem to 'grow' substantially very quickly and the user is motivated to 'invest' more. Often, the scammer pressures the user into downloading technology that allows them to remotely access their electronic devices and accounts, and, in many cases, take out additional loans or credit products.
6. We have also seen scammers encourage the user to purchase cryptocurrency, which means that they cannot get redress under the Payment Systems Regulator's Authorised Push Payment Scams Reimbursement rules.[1]

The impact of these scams on individuals is incredibly detrimental to their overall wellbeing. It is financially, mentally and physically devastating. As the consultation sets out, many are put off from seeking help due to feelings of shame, guilt and embarrassment, so it is hard to get a truly accurate picture of the scale of these crimes.

[1] In addition to the cases reported to us by individual users, Frontier Economics found that the: 'value of APP scams to crypto exchanges has grown significantly, indicatively from around £59 million in 2023 to £153 million in 2025.' See: Frontier Economics, *Independent Evaluation of APP Scam Policies: Summary Report*, 2026, p. 41

Once the scam is taken offline, it is incredibly difficult for a third party to know the actions of the scammer or of the user who is being scammed, and the fraud can go on for months or years. Even after a user realises they have been scammed, some can be contacted by other scammers who will promise to help them 'recover' their money in return for upfront payments. It is absolutely essential that platforms take effective action to prevent scams from being shown to their users in the first place – this is the only way to ensure users will not encounter them and go on to face these devastating outcomes.

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

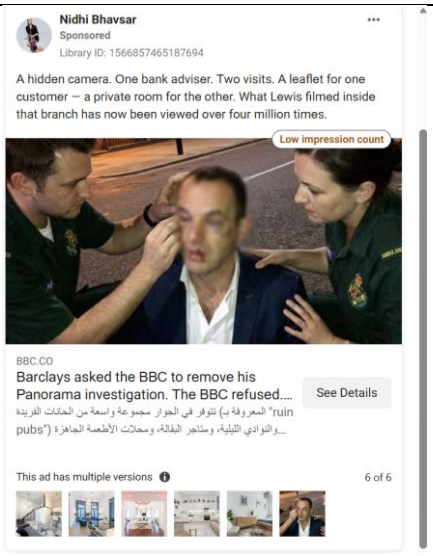
Yes, MSE frequently encounters fraudulent ads that feature almost all the risky characteristics identified (we are unable to evidence cloaking, as we are unable to widely test landing pages).

For example, a typical Martin Lewis scam ad will show an impersonation of his likeness which, when clicked on, takes the user to an unusual URL. The recent trend is for Martin to be in a confrontation with another public figure, for example, the Governor of the Bank of England, Elon Musk, Piers Morgan, a bank CEO or an MP on the 'set' of Question Time. The ads feature exaggerated and attention-grabbing claims that Martin has 'uncovered' some sort of 'secret' to tell the public, which we call 'wealth-loophole' scams.

The advert will often be for a so-called financial investment or crypto related scam – though this is sometimes hidden on initial view of the ad and only discovered when redirected to the destination URL. In the past few years, we have seen a significant increase in the use of Generative AI (GenAI) and deepfake scams – combining Martin's likeness on video with a deepfake of his voice – which are becoming progressively more sophisticated.

In addition, we have observed a recent trend of scammers using multiple versions of ads. For example, an account may post an ad with six versions, five of which link to a legitimate website, with the final version being a scam ad (see example in table 1, below).

Table 1: Examples of fake ads MSE has seen featuring the specified 'risky characteristics'

Characteristics	Ad
• Impersonation of public figures: Martin Lewis and Andrew Bailey. • Use of GenAI to manipulate images of an event that did not happen. • Pressure-inducing content: 'Watch what Martin exposed before your chance is gone.'	
• Impersonation of public figures: Martin Lewis and Piers Morgan. • Unusual URL redirect: alcatelmobileus.org. • Use of GenAI to manipulate images of an event that did not happen. • Attention grabbing: 'Viewers didn't see this coming.'	
• Impersonation of public figures: Martin Lewis. • Unusual URL: https://kidersonesalo.info/ combined with an indication that it is taking you to a BBC website. • Use of GenAI to manipulate images of an event that did not happen. • Attention grabbing: Barclays asked the BBC to remove his Panorama investigation: The BBC refused.	

• Multiple versions of the same ad, with only one version being an obvious scam ad.	

Approach to Codes

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

We agree with the layered approach taken in these draft Codes, which would provide much-needed friction throughout the whole process, from account creation to ad publication.

MSE wants to see Ofcom undertake a review no more than one year after implementation, to ensure the approach has had the desired effect, as the criminals who act within this ecosystem are far more nimble than the platforms' response to them. This review should assess whether the Codes are as effective as hoped and consider if they need to be strengthened. Ofcom should also assess whether its categorisation of platforms is still appropriate, and crucially whether scammers have moved to a platform that is not in scope of the OSA.

The layered approach

It has been well established by Ofcom's research (as well as the evidence submissions of MSE and other concerned groups) that the paid-for advertising ecosystem contains several touchpoints for intervention against fraudulent advertising that are not currently being utilised.[2] We strongly support Ofcom's approach to emphasise the role of account verification (while of course considering the whole picture) and we agree this

[2] See: *MSE Response to the Online Advertising Consultation (DCMS)*, June 2022; *MSE Response to Third phase of online safety regulation: Additional duties for categorised services (Ofcom)*, May 2024

should significantly bolster the barriers to entry and stop more bad actors getting through.

But we would like to see this pre-checking process go further. To add an extra layer of prevention, we propose Ofcom mandates that platforms screen all ads for potential fraud indicators *before* they go live. This step would complement more stringent account verification by acting as a final safeguard. If any fraudsters do slip through the net and successfully set up an account (or take one over), screening all ads first would prevent any bad actor from being able to post scam ads at all, meaning users will not encounter them. We have always maintained this pre-screening should be undertaken by humans if no technological solution exists, though we do believe the major platforms are likely to already have technology capable of assessing whether an ad is fraudulent.

We strongly welcome the proposal to pre-screen all ads for financial services content, and we see this as an indication that the technology exists to screen more widely for *any* illegal, fraudulent content. We look forward to discussing this further as part of the upcoming consultation on Proactive Technologies expected in the Autumn.

Safety by design

We also welcome the proposals around embedding protections from the outset to create safety by design. Financial service providers, which are the last line of defence for individuals transferring money to scammers, already have many of these governance processes in place – so it follows that platforms, who are at the origin of the fraud, should too.

It is crucial that platforms understand how fraud manifests on their services, particularly as many have said that they already implement systems and process to reduce fraudulent content. Clearly, current efforts are woefully inefficient in dealing with this problem, so platforms should undertake an honest and in-depth review to identify weaknesses in their existing systems. For some, this will involve not only an update of systems, but also a culture shift of how they view users' safety – profits should not be prioritised above the financial, mental and physical wellbeing of their users.

Going forward, we would also like to see increased information sharing between platforms, banks and other experts. We welcome the proposal for providers to ban bad actors from all *their* in-scope platforms if they are found to be acting fraudulently on one. However, we suggest Ofcom could be bolder by extending this proposal to the sharing of details across *all* in-scope platforms. If an advertiser is banned for producing fraudulent content, their name, phone number, bank account details and associated addresses or URLs should all be shared across categorised 1 and 2A providers. These details should be used as part of the proposed verification checks on new advertisers – if there is a match, the prospective advertiser should be immediately banned, and any new information linked to them then shared through the network again.

Details could also be shared with banks to prevent any suspicious payments going to these bank accounts, and experts should be kept updated on any new trends in this space. This sharing culture will become integral as scammers tactics continue to develop in sophistication using GenAI and deepfake technology.

Proportionate measures

Our views can be read in more detail to question 5.

Combined impact assessment

5. **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, the overall burden on providers is broadly proportionate – though we strongly feel that there needs to be more direct liability on the platforms to compensate victims of the crimes they enable. We have seen platforms put their profits above the safety of their users far too many times, so perhaps the only way to force compliance with the new duties is to make it cost more to publish fraudulent ads than platforms make from publishing them.

We are reassured by Ofcom's comment in the consultation that, '[Ofcom] consider that loss of revenues associated with fraudulent advertisements are not a relevant consideration for our assessment.'[3] We feel this is a long overdue approach to tackling this harm: platforms are publishers and they shouldn't be able to simply profit from the harm proliferating on their sites.

As set out in the consultation, it is difficult to predict the impact of savings to individuals who will *not* fall foul of online scams because of these changes. What we can assume however, is that the proportionate impact of one of these pernicious scams on an individual user's long-term mental, physical and financial wellbeing is significantly higher than any cost to the platforms in carrying out these long-overdue actions.

Volume 2: Risk, Governance and Control

Advertising intermediaries

6. **Do you agree with our proposal? Please provide any arguments and supporting evidence.**
7. **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**

[3] Ofcom, *Fraudulent Advertising Codes Consultation, Volume 1: Context*, pp. 73-4

implement safety measures in circumstances where they have insufficient control? Please provide any arguments and supporting evidence.

The major platforms that feature the most scam adverts related to Martin Lewis and MSE (Meta, Google, X) operate their own walled garden advertising ecosystem, so our main campaigning on the OSA has largely focused on these rather than intermediaries.

However, we support the proposal to ensure platforms that use intermediaries do have to use 'all reasonable endeavours' to comply with the codes. Ideally, we would like to see stronger language used for this measure. Rather than proposing platforms 'should work with – **or** require…' them to do so, we would prefer for the standard to simply be a requirement from platforms to their intermediaries. We believe this will prevent those platforms from relinquishing responsibility for compliance and would act as a disincentive for platforms to use this system of advertising to circumnavigate the codes.

While outside the scope of this consultation, we believe strongly that intermediaries and the rest of the advertising landscape (e.g. display ads on news sites) should be brought into regulation. We urge Ofcom to work with the Government to reinvigorate work to bring these into regulation as part of the Online Advertising Programme.

Fraud indicator assessment

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

We agree with the proposal for providers to assess how fraudulent advertising manifests on their services. From our own experience in tracking and reporting fraudulent adverts, we know that different platforms see different trends.

We agree with the logic that platforms must understand the characteristics of fraudulent advertising on their sites to ensure they have targeted and effective mitigations, and crucially to understand how it evolves. We have seen scams evolve in sophistication over the last 10 or so years, from some fairly easy-to-spot fake images to highly sophisticated deepfakes of both Martin's likeness and voice. Scammers will always be looking to move with technology, and ahead of detection tools, so it is imperative that these assessments are used to highlight new indicators proactively rather than waiting for a yearly reassessment.

We have previously raised concerns about the risk of fraud becoming more 'personalised' in future using GenAI, and this is already present through cloaking, which the consultation refers to as a risky characteristic. With that in mind, it's crucial that platforms recognise they may be the only link in the chain with a full awareness of what is on their services – while individual users, groups or regulators may see only a 'cleaned' version of the content that is live. Platforms must proactively communicate

emerging risks and the action they are taking to mitigate against them to other platforms, regulators and expert third parties.

We note that Ofcom sets out that most providers have methods already in place to identify and assess risks (Vol 2, p 38), however we know that these methods are clearly not effective given the sheer range and volume of fraudulent ads proliferating across these services. We therefore trust that Ofcom will ensure providers reassess any methods they use and ensure these are improved to ensure compliance with the new duties.

9. **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?**

We broadly agree with the sources listed, but we want to make it clear that referrals from law enforcement or evidence from trusted flaggers should be used as a **last resort**, as these evidence bases can only be formed after fraudulent ads have been seen as active on platforms and action has been taken to report them. Platforms should instead be using their moderation tools to detect any new technique or behaviour coming through in attempted fraudulent ads, which are stopped from going live by effective blockers.

Governance and accountability

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

Not answered.

Testing advertisement generation tools

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

It is absolutely integral that platforms are not contributing to the proliferation of fraudulent advertising by allowing criminals to create scams using their own tools. If platforms cannot guarantee that their tools will not be used for this purpose, they should not be able to profit from them. This not only harms consumers who may encounter these ads on platforms but harms the reputations of legitimate advertisers who use these tools to create genuine advertisements.

Volume 3: Ensuring account integrity

Account checks and actions

12. 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.

In our response to Ofcom's call for evidence in 2024,[4] MSE called for a uniform policy for advertiser verification across platforms, so we are very pleased to see proposals towards this outcome. We strongly agree with the package of checks proposed as well as the need for platforms to perform multiple checks at a range of times in the advertiser process.

We agree with Ofcom's assessment that platforms' current policies are neither extensive enough nor consistently applied – in our previous submission, we set out our understanding that a prospective advertiser could set up an account with simply a bank card on some platforms. A clear set of checks, performed consistently across platforms, and taking place *before* an advertiser can post an advert are all measures that should create the necessary friction that is so long overdue in this process.

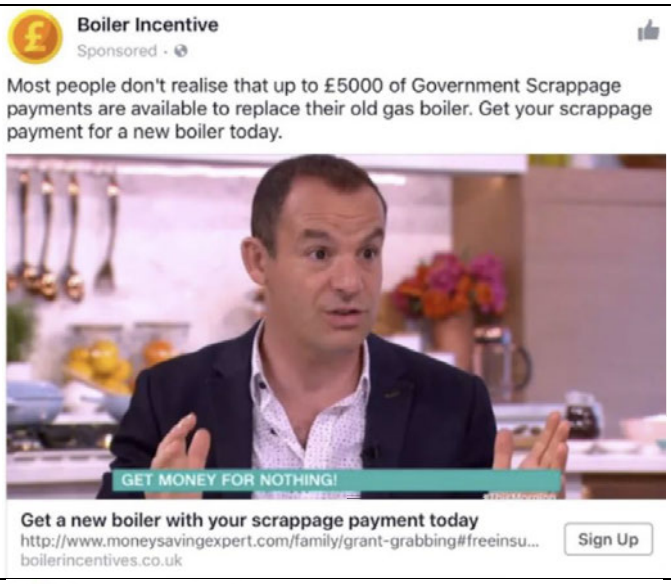
Advertisers who are acting legitimately should have no issue in proving their identity or intentions at each stage, so this should only act as a barrier for bad actors. It is our view that even if the proposals resulted in legitimate advertisers having temporary restrictions placed on them until they could pass these checks, this is still a better situation than the current Wild West of criminals acting with impunity.

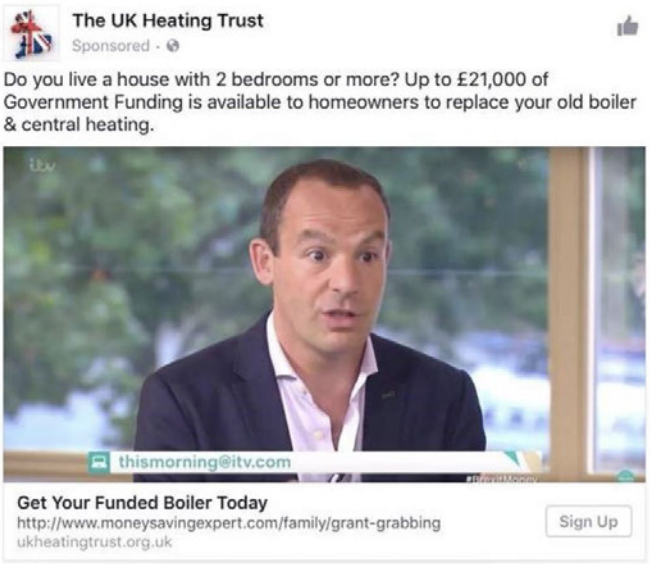
a) Verification of advertising account holders

These proposals seem to be a sensible approach to ensuring an account holder works on behalf of the organisation they claim to be working for. However, we note that on many occasions scammers will use tactics to *suggest* an affiliation with Martin Lewis or MSE, rather than explicitly claim to be working on behalf of us.

[4] *MSE Response to Third phase of online safety regulation: Additional duties for categorised services (Ofcom),* May 2024

Table 2: Examples of adverts that use Martin's likeness and sometimes fake MSE URLs to suggest affiliation with our brand







Our priority ask is for platforms to screen all advertisements before they are published for fraudulent content. We feel it would also be sensible if platforms were required to undertake frequent and thorough checks of an advertiser's content even after verification to ensure that they are only posting adverts with expected content.

For example, if an advertiser has no verified connection to Martin or MSE (none would, as we do not advertise) but is posting adverts with Martin's likeness or MSE's logo they should immediately be banned, all adverts associated with the account removed, and identifiable data shared across in-scope categorised services to prevent them for posting paid-for ads on any service.

b) Repeat checks

We are supportive of repeat checks. Takeover of dormant accounts is a tactic we have seen, so we support the proposals to place checks on accounts that are made live again after a period of inactivity, as a clear indicator they could be being used for fraudulent means.

13. 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.

Not answered.

Preventing fraudulent financial services advertising

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

We strongly support the proposed duties around financial services advertising, particularly the proposal for providers to screen all ads to detect financial services content *before* they go live on platforms, and to ensure the account is appropriately verified to do so. We believe it would be impossible for platforms to fulfil their duty to prevent fraudulent advertising from appearing without this step in the process.

Almost all fraudulent ads featuring Martin Lewis are uncovered to be fake financial services and/or investment scams, exploiting his reputation as a trusted source for consumer finance. It is key, therefore, that accounts posting paid-for advertisements for financial services are rigorously and repeatedly checked for their legitimacy, as we have seen time and time again the financial and mental impact that this type of fraudulent ad can have on individuals, as well as their further economic engagement. As an example, we recently heard from a charity who told us four of their clients had been scammed by a fraudulent Martin Lewis ad – the clients had taken out a total of almost £500,000 in loans between them and face losing their homes, life savings, and have been left with monthly repayments that exceed their incomes. This is just one example of many

devastatingly similar stories we hear because of this epidemic of fraudulent financial service ads.

Again, in the case of a typical Martin Lewis scam, we would like to see any paid-for ad featuring his name or likeness to be instantly detected prior to it being made available to UK users. The paid-for ad should be reviewed, not posted, and, if found fraudulent, the account should be suspended – it should be as simple as that.

We look forward to engaging with Ofcom further on this proposal as part of the upcoming consultation into proactive technologies, but we have always maintained that this does not need to be a technological solution. If there is no technology, then platforms should be forced to undertake a manual check on each and every advertisement that it is being paid to publish – platforms should not be allowed to put their profit margins above their users' safety.

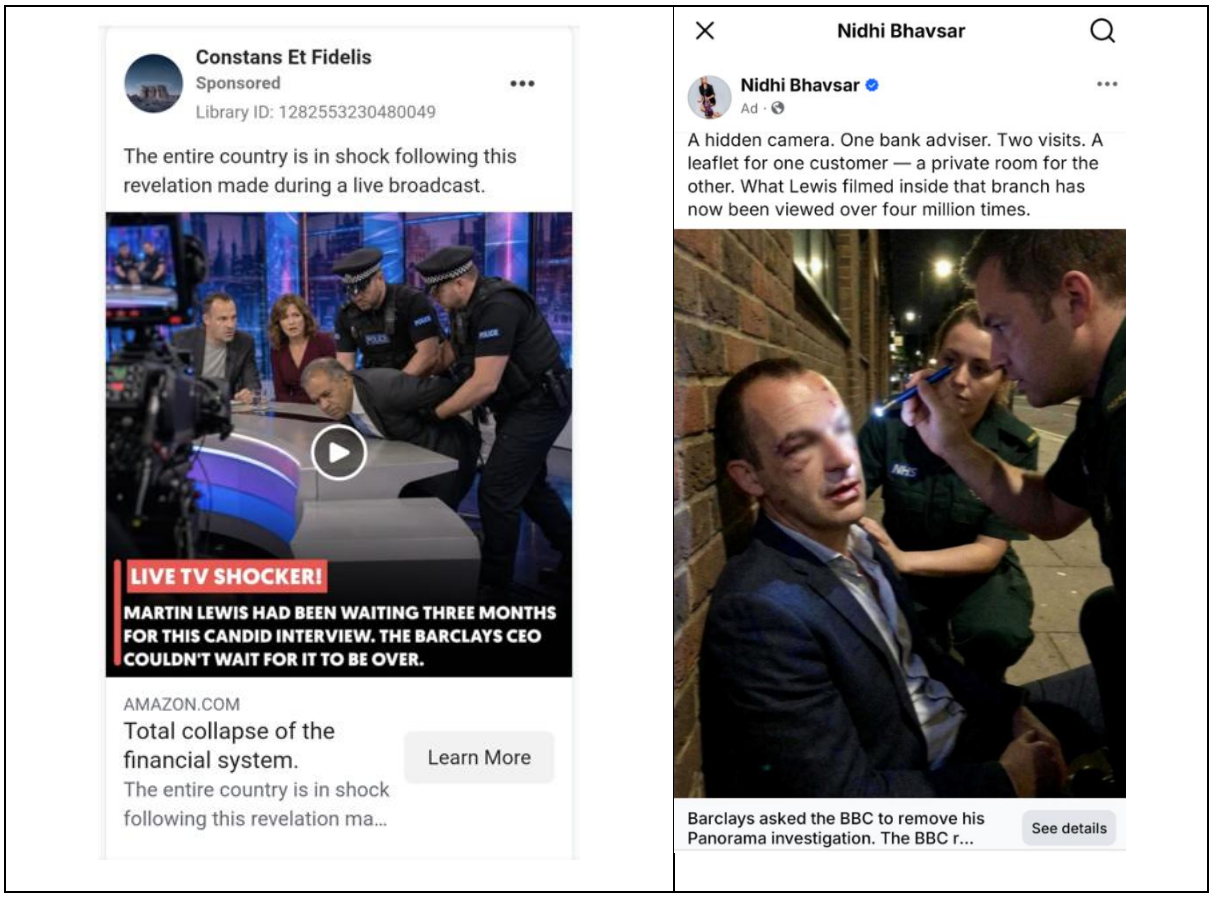
Given that *all* ads would need to be screened in order to detect financial services ads under these proposals, we think it's reasonable for Ofcom to go further and to require that platforms screen for ANY sign of a fraudulent advert across the full range of scams we know appear on platforms. Platforms could use insight gathered from their fraud assessment reviews to benchmark what these signs would likely be. If any are found, these ads need to undertake additional verification before they can be set live.

We have a few further points to raise around this proposal:

1. Destination sites should be checked

Platforms should have to consider and review the content of the destination website as to whether an ad is financial advertising. Most of the scam financial services ads, including many for investment scams which use Martin's image, are not explicit on the face of it that they are for so-called financial products – you only find out from the destination website. In the advert it says things like "This only just happened" or "This was moments ago", combined with AI-generated images of Martin or other prominent figures.

Table three: Examples of fraudulent ads that redirect the user to a fake ad for a financial product, but do not use explicit language about this in the ad



In order for platforms to be able to accurately assess whether the paid-for ad is a financial services ad, it is integral for a holistic approach to be taken – reviewing not just the ad itself that is hosted on the platform, but the content of the page users are being directed to.

2. Scammers should not be able to use exemptions in the FCA's Promotions Order to claim their ads are not for regulated financial services products.

This could pose a particular risk around products which have a high risk of scam activity such as mini-bonds, loan notes and property investments, or adverts from unregulated introducers for these products.

We welcome Ofcom's example 3.3 (P 43, vol. 3), that highlights this as a common tactic for bad actors to use, and that platforms should require evidence from the advertiser that this exemption applies. The Code should make it clear that the High Net Worth or Sophisticated investor exemptions in the Financial Promotions Order are not suitable for mass market platforms, and Ofcom should ensure this is appropriately enforced.

3. Claims Management activity should be included as part of Ofcom's definition of a financial services ad.

It is unclear to us whether adverts from FCA-regulated Claims Management Services will need to be checked in line with the proposals for financial services adverts – we strongly believe they should be. MSE has found social media adverts for Claims Management activity where firms do not appear to possess appropriate authorisation to conduct these activities.[5]

If such activity is excluded, we are concerned that we will see an increase in 'recovery' scams where scammers advertise that they can help people recover losses from fraud and then ask for upfront payments. It would be useful if Ofcom could clarify therefore whether FCA-regulated Claims Management Services are included under the financial services provisions in the Codes.

Countering account takeover

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

MSE agrees with the proposal that providers should implement an account security mechanism on all advertising accounts – we see this as another important layer that applies necessary friction to another stage of the account verification process.

Without the proposals to counter account takeover, we feel it is likely that bad actors will re-double their efforts to take over accounts rather than create new ones, as they are always looking for the path of least resistance. Moreover, we feel that the proposal to have a consistent level of protection across the board ensures that scammers will not be able to take advantage of any one platform with weaker protections.

Overall, these proposals are crucial as part of the package to prevent users from encountering fraudulent advertisements.

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

Not answered.

Advertising bans

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

[5] MSE, 'Live in social housing? Beware shyster firms pretending to be compensation schemes for mould, damp and disrepair', May 2026

We strongly agree that providers should ban advertising account holders that post fraudulent advertisements or fraudulent advertising proxy and take reasonable steps to prevent them from returning to the service.

There is a wealth of evidence to suggest that fraudulent advertisements can be traced back to a small number of account holders.[6] So, it is logical that banning any account that posts such content should reduce instances users encountering scams online.

However, in addition to banning the account holder from the platform where the ad was posted and other in-scope platforms owned by the provider, this proposal should go further to require information sharing between all in-scope categorised services.

There is good reason to suspect an account holder that has been banned from one platform is likely to double their efforts into platforms where they have more chance of getting through, for example a bad actor who has been banned from Facebook and Instagram may focus their activities into X – thus putting X users at a higher risk of encountering fraudulent advertising. Sharing basic information on account holders – such as associated phone numbers, addresses, bank account details – could reduce this likelihood and go much further in protecting UK users online.

We also feel that information sharing between platforms and financial service providers (for example in sharing all known addresses or phone numbers for a bank account) would help providers better meet their objective of taking 'all reasonable steps' to prevent bad actors from returning to the platform. Scammers acting in this space can currently take advantage of the gaps between the origination (i.e. social media sites) and end point (i.e. banks) of their fraudulent activity. Given scammers' ability to adapt faster than regulators to respond, increased data sharing would provide some crucial mitigation against that outcome.

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

Not answered.

Account appeals

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

Not answered.

Volume 4: Moderation

Advertising moderation

[6] Gen, 'The Scam Ad Machine', 1 February 2026

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

Review, assess and remove fraudulent ads

We strongly agree that it is imperative for platforms to have processes in place to review, assess and remove fraudulent advertisements when they are found to be live. It is our view that moderation processes act as a last resort in the process, as ideally platforms would have adequate account verification and pre-screening of ads to substantially reduce the risk of any scams going live on the platform.

Internal advertising policy

We agree that providers should have processes in place to update their policies in response to evidence of new fraud indicators. The consultation sets out that many platforms already have processes in place for the detection and removal of fraudulent advertisements. These processes are fundamentally inadequate given how often users are encountering this illegal content daily.

We have provided evidence throughout the development of these regulations that platforms' internal policies are currently not robust enough to deal with this problem. For example, we have heard from users who have reported fraudulent adverts time and time again, in one case almost a dozen times in a day, only to be told these ads do not break the platform's terms of use.

We agree that the use of a fraud indicator assessment should bolster these internal processes. As we set out in question 8, with scammers constantly adapting their techniques, and the threat of more 'personalised' AI-generated ads, platforms may be the only link in the chain with access to the full picture of this activity. Platforms should therefore be able to build up their evidence base using internal monitoring in the first instance, relying only on reactive third-party flags only to complement – not supplement – this internal work.

Platforms must take this opportunity to drastically improve their internal processes, and Ofcom should not hesitate to take action against those who are not implementing the law.

Performance targets

While we welcome the introduction of targets for the time taken to remove a scam, and the accuracy of a platform's decision making, we are concerned that they are self-determined. Ofcom shouldn't miss the opportunity to set minimum standards for all platforms to meet. Without these, we are concerned that platforms could voluntarily elect to set unambitious targets and artificially inflate their successes. This is particularly the case because the OSA only sets out that platforms must remove

fraudulent adverts 'swiftly' – this is too open to interpretation unless Ofcom better defines what a proactive detection and takedown system looks like.

For example, MSE's own data shows that the median time it takes platforms to remove an ad we have flagged as fraudulent ranges from 1.5 days (Facebook) to 48 days (Instagram).[7] In this scenario, even if Instagram reduced the time it took by 90% it would still leave this content visible, and at risk of defrauding users in the UK, for far too long.

Ofcom should use its extensive evidence base to determine appropriate minimum expectations, for example, by setting the maximum time for a fraudulent ad to be removed at 24 hours, or one hour where it has been reported by a trusted flagger – timeframes we see as reasonable and proportionate given the harm caused in this short time frame.

Prioritisation

We agree that having a prioritisation policy in place should help platforms react proportionately to the biggest threats (i.e. scams with the widest reach), however each individual devasted by the impact of a fraudulent ad is enough reason to take action. A prioritisation policy in place alongside a set of maximum timeframes set by Ofcom would ensure that platforms respond effectively to all scams on their service.

Resourcing

We agree with the proposal to ensure platforms are appropriately resourced to give effect to the measures on internal advertising policies and performance targets. As we have consistently maintained, we believe that if employing individuals to pre-screen each ad for fraudulent activity before it goes live is the only way to ensure scam ads are prevented from appearing on people's feeds, then that is what platforms must do – whatever the cost to resource.

Training and materials

We agree that individuals working in moderation services should receive adequate training and resources. We would like to see a culture within platforms, or at the very least within these teams, that scams should be prevented above profits – if that results in legitimate ads being caught up and subject to appeal, then that is preferable to any scams getting through. The relative harm caused by a legitimate ad being subject to additional screening, versus a fraudulent advertisement tricking an unsuspecting consumer out of thousands of pounds, is simply not comparable.

Terms of service and publicly available statements

[7] Internal MSE reporting data, sample of 12 months

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

Not answered.

Advertising complaints

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

While we agree that reporting tools are a key part of any package of solutions to deal with this harm, such tools should only be seen as a last resort to catch any scam ads that have slipped through the net. The onus should be firmly on platforms to prevent ads from appearing, rather than (as it is now) for consumers and organisations to take action when they come across them.

MSE welcomes the proposal for platforms to have reporting systems and processes that are easy to find, easy to access and easy to use. However, we are concerned that Ofcom's approach to allow flexibility for providers here does not adequately deal with the issues with the current reporting tool landscape. We would like to see more prescription around these tools so consumers have a similar (or ideally, identical) experience reporting across platforms – this will empower consumers to use these tools, and in turn help platforms to fulfil their duty to swiftly remove such content.

We recommend that reporting tools:

- Have the same method for reporting – for example being able to report a specific ad with one click, without the need to be signed in or to give out personal details.
- Use consistent language and symbols across all platforms.

In addition, platforms should better communicate outcomes to those who report a fraudulent ad – whether it is a trusted flagger, other third party or individual user. Reporters should not have to re-engage with the platform to check on the status of a complaint, and platforms should have to explicitly explain why any reported ads were not removed, to demonstrate transparency and accountability within the process.

There should also be a requirement for platforms to tell all users who have clicked on a fraudulent ad that they have encountered one. This could include a clear notification that "you clicked on a fraudulent advert on our platform" with warnings about the behaviour consumers should avoid (such as downloading software enabling remote access) and action they can take such as not making any further payments and reporting the fraud to their bank and Report Fraud.

These proposals for warnings would help prevent fraudulent advertising by increasing the reputational incentives for platforms to prevent ads in the first place. This could also help reduce the returns received by the scammer and their incentives to post ads again.

Ad libraries

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

We strongly support the proposal that all in-scope providers have a publicly available ad library, particularly as there is such a range of approaches. For example, our team has found Meta's ad library in its current form useful for identifying and reporting fraudulent advertising which purports to be of Martin Lewis and/or MSE (though we set out below how it should improve). Meanwhile, X does not have any form of ad library in the UK.

Ad libraries are crucial for flaggers like MSE to detect fake ads – especially as social media feeds become much more personalised, with ads increasingly targeted to specific audiences. Without such libraries, it is impossible for any third party to see what adverts have been published by platforms.

Following implementation, libraries will also be an important tool for accountability, assessing whether platforms are following the Codes and the overall effectiveness of the duties under the OSA.

24. 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.

We agree with the principles that ad libraries should be publicly available, accurate and reliable. As we set out in our response to question 23, MSE frequently uses Meta's library to detect and report fraudulent adverts. It is crucial the library is a) updated in real time, so there is minimal delay between an ad being posted (with users encountering it) and the ability to review and, if necessary, report the ad, and b) is reliably available, as we have unfortunately had to ensure that MSE teams are regularly checking for new fraudulent adverts featuring MSE or Martin's likeness.

The functionalities set out are a welcome start to setting minimum expectations on platforms' ad libraries, but we would like to see these go further by also ensuring that the information categories are also searchable within the library.

It would be most helpful to MSE, as a frequent target of these fraudulent ads, to be able to search by image or by destination URL. Many MSE users send screenshots of fraudulent ads they've encountered on platforms, which means these are the only details we have to identify ads. Currently, this makes it difficult for us to find the ad in an ad library (where one exists), and therefore very hard to flag to a platform for takedown. An ad library that allows for an image search and destination URL is the best solution to help us report these ads.

Many fake images and links are used repeatedly across ads – we noted one deepfake scam purporting to show Martin Lewis 'in conversation' with Elon Musk recurring for

more than 10 months. A searchable repository of these images and links would also allow us to report the same fraud in bulk. Ideally, platforms would use these reports as flags for their pre-screening checks and immediately block any drafted advert featuring either the image or URL from going live and banning the advertiser for fraudulent activity. Both outcomes would reduce fraudulent advertisements on platforms by a) reducing the time a scam is live if it's slipped through the net and b) preventing users from encountering known scams if the content is recycled.

It is also important that all versions of an advert are searchable in the ad library. We have encountered problems trying to search ad libraries for the text in the alternative versions of an advert. This makes scam ads harder to detect and could be one of the reasons some fraudulent ads are missed, like the example we included in our answer to question 1. Ofcom should ensure that this gap in the searchability function is closed.

We also strongly recommend that ads are kept in the library for more than 1 year, ideally at least 3 years, to account for the fact that financial scams can take place over a sustained amount of time. Users who have fallen foul of a scam, particularly a complex financial fraud, could need time to seek help and support after realising what has happened – keeping a record of ads for a longer amount of time means it is more likely they can be used as evidence in these cases.

In addition, we ask that all images associated with the advert are shown in the library. Using Meta's library as an example, adverts that have been found to breach its terms do not show the image as reported – making it difficult for both flaggers and users to check what was removed. These images are useful to use as evidence of a scam for individuals but also allow us to track emerging trends that we can warn our users about.[8] Instead of removing the image from the library, there should be a clear flag on the advert that highlights it has been reported as fraudulent, as well as information on what action has been taken in response to the report.

25. 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?

Not answered.

[8] See MoneySavingExpert.com, 'Martin Lewis scam adverts', updated June 2026

About MoneySavingExpert.com

MoneySavingExpert.com (MSE), founded and chaired by Martin Lewis, is dedicated to cutting consumers' bills and fighting their corner. It is the UK's biggest and most trusted consumer website. For 20 years, campaigning journalism has been at the heart of MSE's mission. The site is behind many notable campaigns, including student finance reform, reducing energy bills, mortgage help, scam ads regulation and helping consumers reclaim an estimated £1bn in bank charges and £12bn in PPI payouts.

With millions subscribing to receive the weekly MSE Money Tips email and visiting the site monthly, MSE ranks as YouGov's most recommended brand (all sectors) in the UK. It is also, according to *Press Gazette,* the UK's largest specialist online news publication, with more traffic than many national newspaper sites. In September 2012, the site joined the MoneySupermarket Group PLC (now MONY Group PLC).

In the event of any queries, please contact the campaigns team:
campaigns@moneysavingexpert.com