Fraudulent Advertising Codes Consultation

Volume 3: Ensuring account integrity

Consultation

Published 10 July 2026
Closing date for responses: 02 October 2026

For more information on this publication, please visit ofcom.org.uk

Contents

Section

1. Ensuring account integrity (Volume 3) – Introduction

1.1 In this volume, we explain our proposals designed to raise the bar on account integrity. Specifically, we are proposing a range of measures to better ensure service providers take sufficiently robust steps to check that advertising account holders opening and operating accounts are not bad actors, that when bad actors are identified they receive an appropriate ban, and that legitimate advertising account holders can quickly and easily report suspected account takeover.

1.2 This volume is structured as follows:

- **Section 2, 'Account checks and actions'** explains our proposals for how service providers can better understand whether an account may be operated by bad actors and how providers can take preventative action to protect users.
- **Section 3, 'Preventing fraudulent financial services advertising'** explains our proposals that service providers check that any firm or individual intending to advertise financial products is legally permitted to do so.
- **Section 4, 'Countering account takeover'** explains our proposals for service providers to have a robust account security mechanism on advertising accounts to prevent bad actors from taking them over to disseminate fraudulent advertising. Where an account has been taken over, we are also proposing providers have an effective mechanism for legitimate advertising account holders to report suspected account takeover.
- **Section 5, 'Advertising bans'** explains our proposals that service providers ban advertising account holders that have posted fraudulent advertising, preventing them from advertising to UK users. They should also take reasonable steps to prevent banned advertising account holders from returning to the service through new and existing advertising accounts.
- **Section 6, 'Account appeals'** explains our proposal on how providers should implement account appeals systems and processes for all advertising account holders that have had action taken on their account.

2. Account checks and actions

What is this section about?

Checks on advertising accounts help service providers understand whether there are risks they are operated by bad actors. Providers can then take action against these accounts. This should enhance the preventative steps providers take to protect users from encountering fraudulent advertising.

In this section we set out our proposed measure about account checks and actions, and why we are proposing to recommend it.

Our proposal

Number in our Codes	Proposed measure applicable to providers of Category 1 and 2A services
FAU H1 and FAS H1	Providers should **have and consistently apply an account checks and actions policy**. It should set out how they: **verify account holders work for, or on behalf of, the individual or organisation they advertise; carry out checks to prevent banned advertising account holders returning; and find accounts with risks they will post fraudulent advertising** to apply restrictions to them. Providers should publish a summary of this policy and review and update their policy at least every 12 months.

Why are we proposing this?

We provisionally consider that robust account checks and taking effective account-level action are essential to prevent users encountering fraudulent advertising, in accordance with providers' duties under the Act.

We are proposing specific checks that we think can be particularly effective to prevent impersonation fraud and prevent banned advertising account holders returning. We are also proposing checks and restrictions that service providers should apply to advertising accounts to assess and mitigate risks. Additionally, we consider that checks should take place to verify if accounts advertising financial services can lawfully do so (these proposals are described separately in Volume 3, Section 3, 'Preventing fraudulent financial services advertising'). This package of steps is designed to make it harder for fraudsters to access service providers' advertising platforms in the first place.

Consultation questions

- 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.

- 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.

Introduction

2.1 This section proposes that providers of Category 1 and 2A services (providers) establish an 'account checks and actions policy' which sets out the checks and actions the provider will carry out on advertising accounts, including the specific checks proposed here.[1] The policy should set out the steps providers take to carry out these checks and the actions they will take to mitigate associated risks. Providers should apply the policy consistently, carrying out the checks and actions as set out in the policy in practice.

2.2 We explain how the proposed measure would work, before setting out our views about why we consider it to be proportionate for service providers to carry out.

2.3 In developing this proposal, we have drawn on evidence from due diligence practices across sectors and from analysis about the types of fraudulent advertising harms service providers should address more effectively. We have also examined current practices and deficiencies in account checks processes and online advertising placement, particularly in integrated ('walled garden') systems. We intend that these proposed measures act as a framework for providers to ensure more robust account-level checks are carried out, using sector-appropriate best practice to reduce the risks and impacts of fraudulent advertising.

2.4 We acknowledge that a Category 1 or 2A service may be serving paid-for advertisements to its users through different advertising pathways. Where relevant, the proposed advertising intermediaries measure would apply. The proposed advertising intermediaries measure recommends that a provider should use all reasonable endeavours to implement a version of any measures it has been unable to apply. For more information, see Volume 2, Section 2, 'Advertising intermediaries.'

Account checks and actions policy

Explanation of the proposed measure

2.5 This sub-section explains our proposed account checks and actions policy measure, which we have split into three components:

- the expectation for service providers to have and apply an account checks and actions policy;
- specific account checks and actions the policy should include; and
- development, regular review and update of this policy.

Having and applying an account checks and actions policy

2.6 Service providers should have a policy detailing the account checks and account actions they carry out on advertising accounts before the paid-for advertisements they post are able to be encountered by UK users.[2] As detailed in paragraph 2.8, some of these checks should relate to specific circumstances or types of paid-for advertisements. Providers

[1] See Annex 7, 'Glossary' for our definition of 'advertising account'.
[2] See Annex 7, 'Glossary' for our definition of 'post or posting an advertisement'.

should apply all checks outlined within the policy consistently. The systems and processes providers have, and the actions they take, should reflect what is set out in their policy.

2.7 We propose to recommend that service providers publish a high-level summary of their account checks and actions policy. This is important to ensure that advertising account holders understand the main elements of the policy and so that there is transparency about the steps the provider is taking.[3] We recognise that publishing too much detail could assist bad actors by revealing how checks operate. We therefore expect providers to share information at a sufficiently high level, without disclosing details that could be misused.

2.8 At a minimum, the provider should carry out the following checks and actions, and the account checks and actions policy should explain how service providers do them:

- verification that advertising account holders work for, or on behalf of, the individual or organisation being advertised, to help prevent impersonation;[4]
- checks and actions to prevent banned advertising account holders returning;
- checks for accounts with indicators that there is a material risk they will post fraudulent advertising and how restrictions will be applied in such cases;[5] and
- repeat checks that are triggered where the provider no longer has confidence that an existing check remains accurate or where there are relevant changes identified on an advertising account.

2.9 We set out our expectations for each of these checks and actions, including the circumstances under which service providers should carry these out, in paragraphs 2.15 to 2.53.

2.10 As set out in Volume 1, Section 3, 'Online advertising ecosystem', paragraphs 3.19 to 3.20, there can be a variety of account hierarchy structures used in online advertising. Depending on the circumstance, it may be more appropriate to carry out the check on a single advertising account holder, multiple advertising account holders, or the advertising account more generally.

2.11 Figure 2.1 provides an illustration of how these checks work together. Providers can carry out checks and actions in whatever order is appropriate for their service, as long as they are applied to all new advertising accounts before paid-for advertisements posted by the accounts are able to be encountered by UK users on the service. For example, a provider may want to carry out checks for banned advertising account holders first so it can take action against them without having to carry out the other checks, or it may conduct them simultaneously.

---

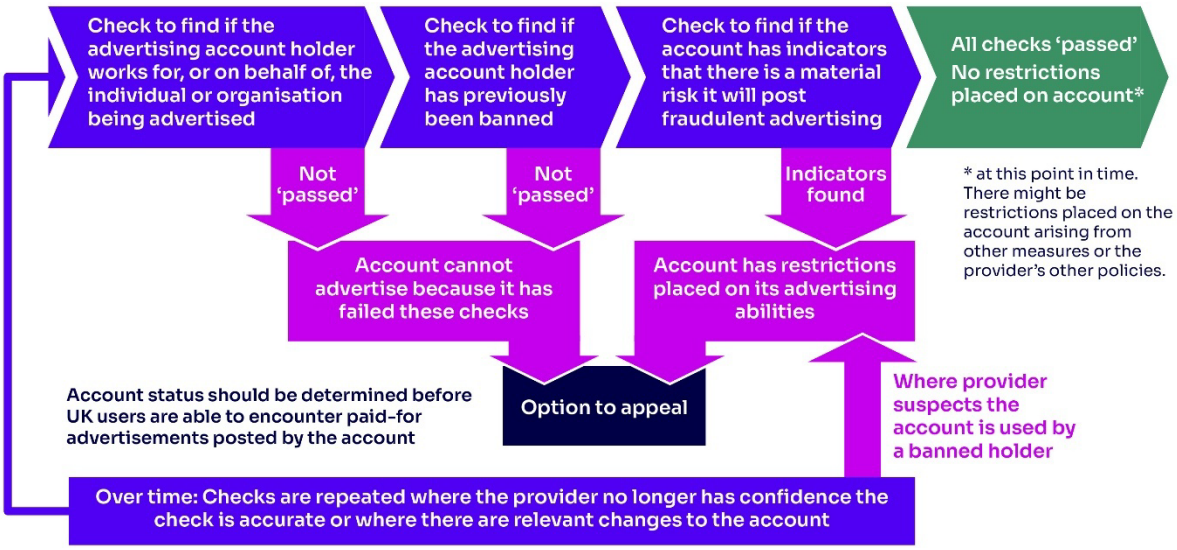
[3] See Annex 7, 'Glossary' for our definition of 'advertising account holder' and Volume 1, Section 3, 'Online advertising ecosystem' for more information about the different types of persons who may use an advertising account. For the purpose of this measure, this also applies to prospective advertising account holders attempting to set up an advertising account including where an existing account on the service is looking to add advertising functionality.

[4] In this section, we use the term 'verification' to refer to the process of checking that something is true and accurate, often using specific evidence to confirm this.

[5] Service providers may place restrictions on an advertising account to reduce the risk they pose to users. This restriction should last until the provider is satisfied the risk of an account posting a fraudulent advertisement has been mitigated. The restriction may be in relation to what the account can do or consist if pre-moderating paid-for advertisements from that account. For more information, see paragraphs 2.42 to 2.47 of this section.

2.12 This means that advertising account holders may be subject to checks at multiple stages before their first paid-for advertisements are able to be encountered by UK users on the service.

Figure 2.1: Account checks and actions flowchart



2.13 We also outline in paragraphs 2.48 to 2.53 our expectation that service providers set out the circumstances where they repeat any of these checks or apply them to accounts which existed before the Fraudulent Advertising Codes come into force.

2.14 Where an advertising account holder has their ability to advertise on the service impacted due to the outcome of a check, we propose that they can appeal this decision. The proposed Account appeals measure (see Volume 3, Section 6, 'Account appeals'), sets out the proposed measure to enable this.

Specific account checks and actions the policy should include

Verification that advertising account holders are working for or on behalf of the individual or organisation they are advertising

2.15 We expect service providers to verify that advertising account holders work for, or act on behalf of, the individual or organisation they are advertising. Providers should carry this check out on all new advertising accounts before UK users are able to encounter the paid-for advertising they post on the service.

2.16 Where a service provider is unable to confirm an advertising account holder passes such verification, the account they use should not be able to advertise to UK users.

2.17 Providers should set out in their account checks and actions policy:

a) how they will understand what the relationship is between the advertising account holder and the individual or organisation they are advertising; and
b) how they will verify that the advertising account holder does work for or on behalf of the individual or organisation they are advertising.

Understanding the relationship between the advertising account holder and the individual or organisation they are advertising

2.18 We firstly expect providers to understand the relationship that the person setting up the account has with the individual or organisation they are advertising. We recognise the

relationship may be with a single organisation they work for, or multiple clients if they work for an advertising agency.

2.19 If an advertising account holder advertises on behalf of a retailer, and that retailer promotes products from multiple brands, providers should consider the relationship as being with the retailer. For example, in the case of a supermarket advertising products, the relationship is with the supermarket rather than the individual brands of the products.

2.20 A single method may be sufficient to understand the relationship, but it may not be appropriate to rely on one method in all circumstances. We expect the steps service providers take would likely include at least one of the following, or a similar alternative:

- Providers could ask advertising account holders what their relationship is with the individuals or organisations they will advertise and who they are.
- Providers could assess details that the advertising account holder wants to display in a user-facing profile presented alongside advertising content, where services have user-facing profiles. Providers may enable advertising account holders to have a 'profile' that appears alongside the paid-for advertisement. Advertising account holders may want this profile to represent a particular individual or organisation.
- Providers could assess information in the first paid-for advertisement created by the advertising account holder before UK users are able to encounter it on the service. We understand that providers can, and do, review the content of paid-for advertisements before they are able to be encountered by UK users on the service.[6]

Verification the advertising account holder does work for, or on behalf of, the individual or organisation they will advertise

2.21 Secondly, we expect providers to verify that the advertising account holder works for, or acts on behalf of, the individual or organisation they are advertising. This may be achievable through a single check or may require multiple checks, depending on the specific circumstances.

2.22 Service providers may determine which checks are most appropriate depending on the relationship between the advertising account holder and the individual or organisation they are advertising. However, providers must ensure that the checks undertaken achieve the objective of verifying that the advertising account holder does in fact work for, or on behalf of, the individual or organisation concerned. We set out the following examples of how this could work for several different types of relationships:

a) An advertising account holder may work on behalf of an individual or single organisation. We expect providers to verify that the advertising account holder works on their behalf under this proposed measure. Examples 2.1 to 2.4 illustrate methods of doing this.

[6] Evidence from the Integrity Institute notes that verification processes for advertisements and advertisers range from basic algorithmic detection to full manual review. Source: Ofcom and Integrity Institute, 2026. Fraudulent advertising and account integrity: Expert insights on best practice; We also have evidence that most providers enter submitted advertising campaigns into a 'review' phase before UK users are able to encounter the advertisements posted by the account. Source: Ofcom, 2026. Online advertising pathways: qualitative research report.

Example 2.1: Advertising account holder owns contact details associated with the individual or single organisation

The service provider verifies if the advertising account holder can demonstrate they own contact details that can be linked to the relevant individual or organisation they are advertising.[7] This could include ownership of an email address with the domain belonging to the organisation being advertised, or ownership of publicly listed contact details. Publicly listed contact details could be found on the individual's or organisation's website or on reliable public lists like the Financial Services Register for UK authorised financial services firms.[8] The provider uses a one-time passcode to verify ownership of the contact details.

Example 2.2: Advertising account holder's identity can be associated with the individual or single organisation

The service provider verifies the 'legal name' of an advertising account holder that can be associated with the organisation. An advertising account may be operated by an individual listed as a current officer on Companies House, or be named on documentation the provider can request from the advertising account holder.[9] Providers could refer to the UK Government's Good Practice Guide 45 (GPG 45) to understand the steps they could take to verify identity where applicable.[10]

Example 2.3: Advertising account holder's payment details can be associated with the organisation

The service provider uses evidence that the advertising account holder can use a corporate credit card associated with an organisation to verify they are acting on its behalf. Where a payment card is provided, the provider applies payment authentication checks, including:

- analysing the card's bank identification number to identify issuer and card type (for example, whether it is a corporate or consumer card);[11]
- verifying the billing address through an address verification service;[12] and
- confirming possession of the card via card verification value (CVV) checks.[13]

[7] For this to be effective, contact details would need to belong to the entity. Providers should take account of the risk of bad actors attempting using spoofing to circumvent checks.
[8] The Financial Services Register is a public record of firms, individuals and other bodies that are, or have been, authorised by the Financial Conduct Authority (FCA) or the Prudential Regulation Authority. Source: FCA, 2026. Financial Services Register. [accessed 13 March 2026].
[9] GOV.UK, no date. Search the register. [accessed 22 June 2026].
[10] GOV.UK, 2024. How to prove and verify someone's identity. [accessed 13 March 2026].
[11] ISO, 2022. ISO/IEC 7812-1:2017. Identification cards – Identification of issuers – Part 1: Numbering system. [accessed 22 May 2026].
[12] Stripe, 2023. What is address verification service (AVS)? [accessed 22 May 2026].
[13] Stripe, 2025. What card verification value (CVV) is – and how it helps businesses prevent fraud. [accessed 22 May 2026].

A nominal transaction may also be used to confirm the card is active and under the advertising account holder's control.

Example 2.4: Advertising account holder demonstrates control of an advertising web domain

The service provider verifies that the advertising account holder has a level of control over a web domain linked to the individual or organisation the advertising account is advertising. The service provider may generate a unique, time-bound verification code that the advertising account holder can then add to the domain name system (DNS) configuration as a TXT record. The service provider can then verify the existence of this DNS TXT record and the correct verification code to establish that the advertising account holder has sufficient control over the advertising web domain. This can be used to evidence that the advertising account holder is associated with the individual or organisation they are advertising.

b) An advertising account holder may post a paid-for advertisement for themselves as an individual, for example, to sell a single product or service they offer. In this case, the advertising account holder is advertising on behalf of themselves, and so the most appropriate method is likely to involve verifying the identity attributes of the individual advertising account holder. This is illustrated in Example 2.5.

Example 2.5: Verifying the 'legal name' of an advertising account holder

The service provider verifies the 'legal name' of an individual advertising account holder. The provider refers to the UK Government's GPG 45 to understand the steps they could take to do this.[14]

c) An advertising account holder may advertise for multiple organisations, for example, because they work for an advertising agent. We expect providers to verify that advertising account holders act on behalf of at least one of the organisations they are advertising. Example 2.6 illustrates a method of doing this.

Example 2.6: Vouching

Where the advertising account holder claims to be an advertising agent, the service provider asks which individuals or organisations they are advertising, or for information that could provide these details like the agent's website. The provider makes contact with at least one of these organisations to ask them to vouch that the advertising account holder is an agent acting on their behalf or share information like a contract, ensuring the source is sufficiently reliable.[15] [16] The provider then has confidence the

[14] GOV.UK, 2024. How to prove and verify someone's identity. [accessed 13 March 2026].

[15] For example, the verification used in Google's Business Message verification: "When you verify an agent, Business Messages confirms the agent's information with a contact from the brand that the agent represents. Once the brand contact confirms that you can represent the brand with the agent and that the agent information is correct, the agent is verified". Source: Google for Developers, 2024. Business Communications, Business Messages. [accessed 13 March 2026].

[16] The UK Government has also produced guidance about how vouching can be used to verify a claim. Source: GOV.UK, 2020. How to accept a vouch as evidence of someone's identity. [accessed 13 March 2026].

agent is acting on behalf of the relevant organisation and is likely to also legitimately advertise for other organisations.

2.23 The methods set out in examples 2.2 and 2.5, as well as other methods providers might use, could involve identity verification using ID documents (for example, passport or driving licence). We set out our consideration of such checks in paragraphs 2.89 to 2.92 under 'Benefits and effectiveness'.

Checks that providers carry out to prevent banned advertising account holders returning

2.24 Service providers should carry out checks to determine whether new accounts have been set up by banned advertising account holders. These should be carried out against all new accounts before UK users are able to encounter the paid for advertising they post on the service.

2.25 Under our proposals for advertising bans, set out in Volume 3, Section 5, 'Advertising bans', sub-section 'Preventing return', providers should carry out account checks as part of the reasonable steps they take to prevent banned advertising account holders returning to the service. Providers should set out how they do this in their account checks and actions policy.

2.26 At a minimum, service providers should carry out these checks in two stages:

- collecting information about all holders of new advertising accounts before UK users are able to encounter the paid-for-advertisements they post, so that providers are able to build a picture of who they are; and
- checking this information against information they have about banned advertising account holders.

2.27 When a new account is set up, and these checks indicate that the account is linked to a banned advertising account holder, the provider should prevent the new account from being set up. This should be done even if any other holders of the advertising account are not subject to a ban. Providers should ensure that relevant information about banned accounts is kept in a format that allows for such checks to take place.

2.28 Information about advertising account holders that service providers may collect when new accounts are set up for this purpose includes:

- contact details, such as account name, email address and phone number;
- metadata, such as IP address and location data;
- information such as payment details; and
- other data collected during account checks for the purpose of account verification.

2.29 Service providers may decide to carry out an identity verification check to verify this information using ID documents (for example, passport or driving licence). We discuss the consideration of such checks in paragraphs 2.89 to 2.92.

2.30 The service provider should prevent advertising account holders from returning to the service where it determines that they have previously been banned.

Example 2.7: Checks to prevent banned advertising account holders returning

The service provider collects payment details, an email address and a phone number from all new advertising account holders. The provider verifies the advertising account holder actually owns the contact details by sending a one-time passcode to them. The

provider also uses a nominal transaction to confirm the card is active and under the advertising account holder's control.

It determines that, to take reasonable steps to prevent banned advertising account holders returning, it should check where any holders of new advertising accounts use payment details, a phone number or an email address used by a banned advertising account holder.

Where an advertising account holder setting up an advertising account attempts to use the same payment details as one that had previously been banned, the provider utilises the systems and processes it has in place and is made aware of this. The provider can then prevent the account from being able to post paid-for advertising on the service that UK users are able to encounter. The provider can also record the contact details used by the new advertising account so that other new advertising accounts using those can also be prevented from posting paid-for advertising aimed at UK users.

2.31 After carrying out these checks, a provider might have varying degrees of certainty about whether an advertising account holder has previously been banned. We want to ensure that providers still take action where a provider cannot conclude, but suspects, that a banned advertising account holder is attempting to return to the service. Providers should treat these accounts as having a risk that they will post fraudulent advertising. We consider that these accounts should be restricted, as set out under 'Applying restrictions to advertising accounts with a risk that they will post fraudulent advertising' in paragraphs 2.42 to 2.47.

Checks for accounts with indicators there is a material risk they will post fraudulent advertising, so that restrictions can be applied to them

2.32 We propose that providers should collect information on all new advertising accounts before their paid-for advertisements are able to be encountered by UK users on their service, to assess whether they have an indicator that there is a material risk they will post fraudulent advertising. Providers should then apply appropriate restrictions to these advertising accounts to reduce the risk they pose to users.

2.33 Service providers should set out in their policy:

a) the checks used to find advertising accounts with indicators that there is a material risk they will post fraudulent advertising; and
b) the type and duration of restrictions they will apply to these accounts, and how the type of restriction reduces the risk they pose to users. The types of restrictions providers should apply, such as limiting spend or restricting advertising reach, are set out in paragraph 2.45.

Designing checks to find accounts with indicators that there is a material risk they will post fraudulent advertising

2.34 Providers should determine the indicators that there is a material risk an account will post fraudulent advertising on their service. In doing so, providers should consider findings from their fraud indicator assessment (see Volume 2, Section 3, 'Fraud indicator assessment'), or any alternative measures adopted to assess indicators of fraudulent advertising on their service. The proposed fraud indicator assessment measure expects providers to understand the indicators of fraudulent advertising on their service, including those at an account level.

2.35 Certain indicators of fraudulent advertising are likely to be present at the account set-up stage. Service providers should ensure that the checks carried out on new accounts, such as

onboarding questions or data collection, are designed to find all accounts which display such indicators.

2.36 We understand these would be specific to each service and set out some examples under paragraph 2.40.

Applying checks to find accounts with indicators that there is a material risk they will post fraudulent advertising

2.37 Service providers should first carry out checks against all new accounts to establish whether they display the relevant indicators. In some cases, a single initial check will clearly suggest whether an advertising account has an indicator that there is a material risk it will post fraudulent advertising. In other cases, a single check will not be sufficient, and so additional checks should be completed. These could be carried out on a subset of accounts depending on the outcome of the initial check. The conclusion of these additional checks should either be that the relevant indicator is present, or that it is not.

2.38 Additional checks would involve service providers checking something about the advertising account to a higher confidence level or checking information about the advertising account, advertising account holders or an individual advertising account holder that has not been checked before. Where providers need to carry out additional checks, they should also do these before UK users are able to encounter advertising posted by the account on the service. We include non-exhaustive examples of such additional checks among the examples set out under paragraph 2.40.

2.39 Service providers may also need to view advertising before users are able to encounter it on the service to effectively carry out additional checks.[17] Certain features of the content, including the landing page the paid-for advertisement links to, could be relevant to indicators that the accounts will post fraudulent advertising.

2.40 We consider that providers are best placed to determine how to carry out such account checks on their service. The following boxes set out a number of illustrative examples intended to support service providers when doing so.

Example 2.8: Accounts that appear to be created by bots

The service provider uses its fraud indicator assessment to determine that accounts which appear to be created by bots indicate that there is a material risk that they will post fraudulent advertising, and that it can find accounts with this indicator.

The provider carries out an initial check to understand the length of time it took for an account to be created, because rapid creation of accounts may indicate that the creation is automated. Rapid account creation might signal that the account will share fraudulent advertising content.[18]

The provider also subjects all accounts to a check that could determine if they are being run by a bot.[19]

[17] For an explanation that we consider this is possible see footnote 6.
[18] See Volume 1, Section 4, 'Causes and impacts of fraudulent advertising', paragraph 4.44.
[19] For example, a CAPTCHA is a Turing test to tell human and bots apart. It is easy for humans to solve, but hard for bots and other malicious software to figure out. Source: Google Support, 2026. About ReCaptcha. [accessed 19 March 2026].

The provider concludes that accounts which may be created by bots (where it is reasonable to conclude this from these checks) indicate that there is material risk that they will post fraudulent advertising.

Example 2.9: Accounts that may be selling fake medical products

'Miracle health scams' and other marketing for medical products are used to defraud users on the service.[20] The provider uses its fraud indicator assessment to determine that accounts appearing to intend to advertise fake medical products indicate that there is a material risk that they will post fraudulent advertising, and that it can find accounts with this indicator.

The provider takes steps to understand if advertising account holders intend to advertise for medical products (or are uploading such advertisements).

The provider consults official lists and subjects those accounts to an additional check to find out if they will advertise for a registered pharmacist or online doctor service.[21]

The provider concludes that accounts that are not advertising for an individual or organisation on these lists appear to intend to advertise for fake medical products and so indicate that there is a material risk that they will post fraudulent advertising.

Example 2.10: Accounts using stolen details

The service provider uses its fraud indicator assessment to determine that accounts being set up using stolen contact and payment information indicate that there is a material risk that they will post fraudulent advertising, and that it can find accounts with this indicator.

The provider collects contact and payment information for all accounts during onboarding.

The provider checks this information against a reputable third-party list of contact and payment information that has been reported as stolen.[22]

The provider concludes that accounts using details listed on these databases indicate that there is a material risk that they will post fraudulent advertising.

---

[20] See Volume 1, Section 4, 'Causes and impacts of fraudulent advertising', paragraph 4.23.

[21] The UK National Health Service (NHS) recommends that where people buy medicines online, they should ensure that any online pharmacy is registered with the General Pharmaceutical Council and any online doctor service is registered with the Care Quality Commission and the General Medical Council. Source: NHS, 2023. Medicines information. [accessed 19 March 2026].

[22] Examples of third-party lists include Cifas's National Fraud Database, which has been used by various sectors for over 30 years. Signal 'clearing houses' like the Global Signal Exchange can also be used by services to find credentials that could be associated with fraud. Sources: Cifas response to the 2024 Call for Evidence: Third Phase of Online Safety Regulation, p.4; Global Signal Exchange, no date. About the Global Signal Exchange. [accessed 1 April 2026].

Example 2.11: Accounts located outside the UK appearing to be advertising a fake business

The service provider uses its fraud indicator assessment to determine that accounts appearing to be advertising for a fake business purported to be established in the UK, but where the advertising account holder appears to be located outside the UK, indicate that there is a material risk that they will post fraudulent advertising. It determines that it can find accounts with this indicator.

The provider collects information about all accounts to understand where they are geographically operated from.[23]

The provider then subjects accounts operated from overseas to an additional check to find out if they are advertising on behalf of companies registered in the UK as they claim. That involves checking if the company is registered through Companies House.[24]

The provider concludes that accounts advertising for companies which are not registered in the UK, as claimed by the advertising account holder, indicate that there is a material risk that they will post fraudulent advertising.

2.41 The methods providers might use to check an advertising account has indicators that there is a material risk that it will post fraudulent advertising could involve identity verification using ID documents (such as a passport or driving licence). For example, doing this as an additional check could help the provider have more confidence about who the holder of an advertising account is. We set out our consideration of such checks in paragraphs 2.89 to 2.92.

Applying restrictions to advertising accounts with a risk that they will post fraudulent advertising

2.42 A service provider should apply a restriction, in line with its policy, to mitigate several kinds of risks:

- restrictions should be applied to advertising accounts found with indicators that there is a material risk that they will post fraudulent advertising (as discussed from paragraph 2.32 to 2.41); and
- providers should also consider when to apply restrictions as part of the reasonable steps they take to prevent banned advertising account holders returning to the service (as discussed in paragraph 2.31).

2.43 The restrictions service providers place on advertising accounts should mitigate the risk they pose to users. Providers should place more than one restriction on an account where this is necessary to mitigate the risk posed by the account.

2.44 The provider should only lift the restriction once it is satisfied that the risks of the account posting fraudulent advertising has been mitigated. Bad actors may adapt their behaviour where they are aware their account has been placed under scrutiny, and this will affect what duration of restriction is necessary to reduce risk to users.

---

[23] Providers should be aware of any limitations in the methods they choose. For example, using an IP address can be limited by the reliability of the geographical IP address location database and the possibility for advertising account holders to change their IP address to appear like they are in a different location.

[24] Companies House is a register of companies incorporated in the UK. The ease with which bad actors can set up a registered company varies between jurisdictions. Providers should therefore be aware that what can be inferred about the legitimacy of a registered company will vary between jurisdictions.

The restrictions providers should apply

2.45 A restriction should involve one or more of the following:

- limiting the amount an account can spend on advertisements within set periods, for example daily or weekly limits, to reduce the volume of advertisements an account can post;
- limiting the number of users able to encounter paid-for advertisements posted by an account, for example, by limiting the number of impressions advertisements can have or the number of advertisements an account can post;
- limiting the ability to target users from particular groups who are able to encounter advertisements, for example, by restricting the ability of an account to target certain audiences;
- restricting the use of certain advertising formats, such as those which are harder to moderate, like videos; or
- reviewing any relevant paid-for advertisements in accordance with the Advertising moderation measure (see Volume 4, Section 2, 'Advertising moderation') before they can be placed on the service by the account.

2.46 The service provider may decide to place a restriction on an advertising account, or on individual or multiple advertising account holders, depending on the risk identified. For example, where indicators of material risk are linked to the actions of a specific advertising account holder, the provider may restrict that individual's access or permissions.

2.47 Providers should maintain a record of all the restrictions they place on accounts, including what the restriction was. We consider that such records should be kept for a minimum of three years (consistent with our Record-Keeping and Review Guidance), or in accordance with the organisation's record retention policies, if longer.[25]

Repeating checks and existing accounts

2.48 Service providers should set out the circumstances in which they will do a repeat check in their account checks and actions policy. We would expect repeat checks to be triggered where providers no longer have confidence that an existing check remains accurate or where there are relevant changes identified on an account. Maintaining a record of outcomes from account checks would support this. Providers may also conduct a repeat check where they have previously placed a restriction on an account and are checking to see if the risk has been mitigated before lifting it.

2.49 Examples of circumstances where repeat checks would be appropriate include where providers have reason to suspect that an account able to advertise to UK users:

- may have been subject to account takeover;
- has changed the type of advertising it posts (for example, starting to post financial services advertisements or another restricted product or service);
- has a change in the individual or organisation the advertising account holder is advertising;
- is held by an agent that may not act on behalf of the individual or organisation it is advertising for (for example, it has begun advertising a better known brand than it has previously, which could be a sign of impersonation);

[25] Ofcom, 2025. Record-Keeping and Review Guidance.

- has become active again after a period of inactivity;
- has been or is seeking to be newly linked to another account; or
- has changed its account name.

2.50 Service providers should consider when other systems and processes on the service would highlight that something should be rechecked. For example, when applying proactive technology, the provider may detect a suspicious advertisement or suspicious behaviour from an account that could indicate account takeover.[26] The account may not have posted fraudulent advertising in this instance, but the behaviour of the account could justify repeating a check under the provider's policy.

2.51 Service providers should determine the circumstances when they will undertake a check on a pre-existing account that posts paid-for advertising that UK users are already able to encounter, because it was created before the provider introduced its account checks and actions policy. Providers may decide to carry out checks on existing accounts in a phased approach, targeting those which are highest risk first. This would be similar to how we understand other sectors, such as the banking sector, focus checks in a risk-sensitive way.[27]

2.52 As set out in Volume 3, Section 5, 'Advertising bans', sub-section 'Preventing return', where service providers have reason to suspect that an existing account is being used by a banned advertising account holder, they should carry out repeat checks against the account. Providers should detail the circumstances in which they will carry out these checks in their policy.

2.53 Where the provider determines that the account is being used by a banned advertising account holder, it should ban the account from the service. Where the service provider suspects that an advertising account may be being used by a banned advertising account holder, they should apply a restriction. We set out types of account restrictions in paragraph 2.45. The provider should ensure that the restriction effectively mitigates the risk of the account being used to post fraudulent advertisements.

Development, regular review and update of the policy

2.54 We expect service providers to review and update their account checks and actions policy to ensure it is, and continues to be, effective at ensuring the checks providers should do are carried out.

2.55 Service providers should consider at least the following when initially developing and reviewing their policy:

- information from the provider's fraud indicator assessment;
- information relevant to account checks made available by internal and external experts in fraud, including trusted flagger reports and reports published by bodies with relevant expertise such as the National Economic Crime Centre (NECC) and the Financial Conduct Authority (FCA);[28]

---

[26] We plan to propose measures on using proactive technology to detect fraudulent advertisements in autumn 2026. Please see Volume 4, Section 2, 'Advertising moderation' paragraphs 2.14 and 2.15 for more detail.
[27] Examples from the UK banking sector include risk-based customer due diligence requirements under the Money Laundering Regulations 2017. FCA, 2026. Sourcebook. FCG Financial Crime Guide: A firm's guide to countering financial crime risks (FCG). [accessed 29 May 2026].
[28] 'Trusted flagger reports' refer to reports made by trusted flaggers as defined in Volume 4, Section 4, 'Advertising complaints', subsection 'Dedicated reporting channels for trusted flaggers to report fraudulent advertisements'.

- trends from previous advertisement moderation decisions in order to assess what combination of checks and account action could reduce the risk of users encountering fraudulent advertising, with providers using their records of restrictions placed on accounts to inform this analysis;
- the service's design or operation in relation to paid-for advertisements, for example, if providers allow paid-for advertising through video format (and any changes made to design or operation since the last review); and
- changes to technology and tactics that can be used by fraudsters and providers, for example bad actors could use advances in the capability of artificial intelligence (AI) to circumvent certain checks, while providers can also use these advances to improve their approaches to reducing fraud, with some describing their use of AI in this way.[29]

2.56 Service providers should use the findings from this review to update their account checks and actions policy. Providers should also update their published high-level summary of their account checks and actions policy as needed.

2.57 Providers should carry out the review and implement any subsequent updates at least every 12 months or if there is a significant change in the way advertising on the service operates.

2.58 A provider should keep a written record of the annual review and of current and previous versions of its account checks and actions policy so that it can track progress and learn from previous reviews. We consider that such records should be kept for a minimum of three years (consistent with UK records management and retention and disposal in our Record-Keeping and Review Guidance), or in accordance with the organisation's record retention policies, if longer.

2.59 Service providers may choose to align their process for developing, reviewing and seeking expert input into their account checks and actions policy, and other processes such as their fraud indicator assessment.

Benefits and effectiveness

2.60 In this sub-section, we first explain the effectiveness of advertising account checks overall, followed by the benefits and effectiveness of the specific checks we are proposing, including the role of identity verification. Finally, we set out the benefits of providers reviewing and updating their policies.

Benefits of account checks

2.61 As outlined in Volume 1, Section 4, 'Causes and impacts of fraudulent advertising', certain characteristics of advertising accounts can indicate that there is a risk they will post fraudulent advertisements. Evidence presented in that section shows that indicators can be identified through sign-up behaviours, such as rapid account creation, and through unusual account changes or patterns, including inconsistencies between paid-for advertisements and an account's stated purpose.

2.62 Where service providers carry out checks to determine whether an account exhibits these characteristics before UK users are able to encounter its paid-for advertisements, they are

[29] London Stock Exchange Group (Flowe, D.), 2024. 2024: The year AI breaks content-based identity verification? [accessed 2 April 2026]; Bawa, J. and Parakh, P., 2025. How we're using AI to combat the latest scams, Keyword, 8 May. [accessed 8 May 2026].

better able to find higher-risk accounts in advance of them causing harm. This allows providers to take account-level action to mitigate risks to users and help prevent the dissemination of fraudulent advertising.

2.63 This is supported by an Integrity Institute insight report which describes checks being among the effective strategies to combat fraud and frustrate fraudster operations.[30]

2.64 Some service providers have also described the role they think checks can play:

- Meta has stated that "the verification process helps promote greater transparency, limiting attempts to misrepresent advertiser identity", and described this as "an important part of our multi-layered approach to help protect people on our apps from scams."[31]
- Google has described its approach to advertiser enforcement, stating that it is "fighting advertiser fraud at scale, using signals like business impersonation and illegitimate payment details", and that in 2024 it suspended "over 39.2 million accounts in total, the vast majority of which were suspended before they ever served an ad."[32]

2.65 However, the Integrity Institute insight report also found that the current checks service providers carry out are not extensive or comprehensively applied, as buying advertisements is often designed to be as 'low friction' as possible.[33] Similarly, Ofcom research found that providers take a range of approaches. Even where checks are carried out, they may only be done after an account's advertisements are able to be encountered by users, and transparency about them is limited.[34] We have designed our proposals to change this and ensure that comprehensive checks and actions are consistently carried out by providers.

2.66 In other sectors there are requirements and expectations for businesses to carry out checks. Concepts used to describe the checks in other sectors include 'know your customer' and 'due diligence'. These are used preventatively to disrupt fraud and other criminal activity. They can involve assessing the risk posed by a customer at the beginning of a commercial relationship; carrying out initial checks about them; and carrying out enhanced checks where needed, such as where the perceived riskiness of a customer changes.

2.67 In its response to our 2024 Call for Evidence: Third Phase of Online Safety Regulation, Which? noted that "KYC [know your customer] checks are an established element of fraud prevention in financial services and would be a useful addition to online services."[35] The NECC have also suggested to us that "Robust KYC checks have been mandated effectively within the banking and finance sector and there is a clear need for a tiered and enhanced approach to the customer due diligence processes within advertising as well."[36]

2.68 In the financial services sector, banks are required by the FCA to carry out risk-based due diligence about their customers to understand who they are and the risks they pose. These

---

[30] Ofcom and Integrity Institute, 2026. Fraudulent advertising and account integrity: Expert insights on best practice.
[31] Meta, 2026. Fighting Scammers and Protecting People with New Technology and Partnerships. [accessed 19 March 2026].
[32] Google, 2024. 2024 Ads Safety Report. [accessed 14 April 2026].
[33] Ofcom and Integrity Institute, 2026. Fraudulent advertising and account integrity: Expert insights on best practice.
[34] Ofcom, 2026. Behavioural audit of services with advertisement functionality.
[35] Which? response to 2024 Call for Evidence: Third Phase of Online Safety Regulation; p1.
[36] NECC, 2025. Advertiser KYC checks. [accessed 28 May 2026].

are often referred to as 'know your customer' checks and are carried out with the aim of preventing money laundering and fraud.[37]

2.69 Additionally, in the telecoms sector, Ofcom has set out that providers should conduct 'know your customer' checks when sub-allocating telephone numbers.[38] This is designed to help ensure that providers know who they are sub-allocating or assigning phone numbers to so they can prevent misuse, including scams.

2.70 The evidence and expert testimony set out in paragraphs 2.61 to 2.69 suggests that measures stipulating that service providers should undertake account checks would be an effective means of tackling fraudulent advertising.

2.71 As set out in Section Volume 1, Section 4, 'Causes and impacts of fraudulent advertising', fraudulent advertising causes harm at significant scale. We therefore consider that introducing an effective account checks measure would deliver material benefits for users by giving providers a framework to optimise and build on their current practice.

Benefits of the specific checks we are proposing

2.72 We recognise that there is no simple solution to fraudulent advertising. Each of the individual checks we propose to recommend is designed to address a specific risk or tactic. Fraud tactics and risks evolve at pace. We consider there are benefits of us not being too specific about the steps of each check, so that service providers can adapt the design of their checks as fraud methodologies change.

2.73 While bad actors may be able to bypass some checks, we are proposing several specific types of check because it introduces friction that can find or deter harmful activity. We consider that a layered approach is likely to be the most effective.

Verification that advertising account holders work on for or on behalf of the organisation or individual being advertised

2.74 As evidence in Volume 1, Section 4, 'Causes and impacts of fraudulent advertising' demonstrates, impersonation is a common tactic used by fraudsters and it can take many forms, such as impersonating brands or public figures.[39] This proposed measure is likely to be most effective against 'impersonation through accounts', but may also prevent some 'impersonation through content'.[40]

2.75 The Integrity Institute insight report has described impersonation as a common threat and detailed that there have been many high-profile impersonation attacks that have caused real financial harm to companies and people.[41] Meta described how a criminal scam

---

[37] Experian (Sewell, T.), 2024. What is KYC? Support compliance with 'Know Your Customer' Checks. [accessed 19 March 2026].
[38] Ofcom, 2022. Good Practice Guide to help prevent mis-use of sub-allocated and assigned numbers.
[39] For an explanation of evidence about impersonation beyond what is set out in this section, see Volume 1, Section 4, 'Causes and impacts of fraudulent advertising', subsection 'Risky Characteristics'.
[40] There may be similarities between the processes providers use to comply with this proposed measure, and the 'Notable and monetised labelling schemes' measure in the Illegal content Code of Practice for user-to-user services (where the measure applies to the service). This is because they may both involve providers checking an advertising account holder's claimed relationship with an organisation or individual. Providers should determine the circumstances in which it is appropriate to layer on other processes. Source: Ofcom, 2024. December 2024 Statement on Protecting People from Illegal Harms Online, Volume 2: Service design and user choice.
[41] Ofcom and Integrity Institute, 2026. Fraudulent advertising and account integrity: Expert insights on best practice.

syndicate impersonated "government officials, law enforcement, regulators, attorneys, or advocacy organizations with promises to help those who have been previously scammed recover their funds." This included impersonation of these organisations in accounts used to post paid-for advertisements.[42]

2.76 Ofcom research also found that users were more likely to trust adverts from well-known established brands that they were familiar with. This suggests that where bad actors feature a well-known organisation in fraudulent advertising, such as brands or a public body, they are more likely to cause users to fall victim to it.[43]

2.77 Where service providers verify that advertising account holders work for or on behalf of the individuals or organisations they advertise, they will likely be better able to prevent impersonation fraud. Given the prevalence of impersonation fraud and its effectiveness as a tactic, we provisionally consider that this type of verification should deliver clear and material benefits in reducing the incidence of fraudulent advertising.

Checks to prevent banned account holders returning

2.78 We explain in Volume 3, Section 5, 'Advertising bans' the benefits of providers banning advertising account holders who have posted fraudulent advertising on the service. We also set out in that section that the effectiveness of advertising bans also depends on how easily bad actors can evade them. This is why we expect providers to take reasonable steps to help prevent banned advertising account holders returning to the service.

2.79 We consider the account checks we are proposing providers carry out to prevent a banned account returning would be effective in protecting users and reducing the overall volume of fraudulent advertising appearing on the service. We think that both steps we expect providers to carry out are necessary for the proposed measure to be effective as:

- Collecting information about all new advertising account holders before their advertisements are able to be encountered by users is important to make sure advertising account holders can be traced. If providers do not do this, bad actors could post fraudulent advertising which is encountered by users on the service before the provider has collected information about them. The provider would then be less able to effectively enforce the subsequent ban on the account.
- Checking this information against information held on banned advertising account holders can help prevent bad actors from returning during account creation. Account creation is an important opportunity for providers to identify and stop previously banned advertising account holders before they cause further harm to users. Comparing information collected about new accounts with those of banned accounts is an effective way to identify attempted re-entry, including where the information matches or otherwise suggests that a banned advertising account holder is seeking to return using a new account.

[42] Meta, 2026. Adversarial Threat Report: First Half 2026, pp.18 and 19. [accessed 8 April 2026].

[43] Our research also shows that some users may pay attention to 'verified account badges' when deciding whether they can trust an advertisement. If providers use 'verified' badges, without actually verifying the relationship between the advertising account holder and the individual or organisation being advertised, this could increase the risk of users falling victim to impersonation fraud. Source: Ofcom, 2026. Online paid-for advertisements research.

2.80 Service providers may be part of initiatives or commitments to share information with each other or other parties.[44] These include the Global Signal Exchange, which enables organisations, including service providers, to share 'signals' with each other.[45] We consider that the account checks we are proposing will strengthen the accuracy, consistency and overall value of any information providers share about bad actors. If a provider is part of such initiatives, it could also strengthen the range of information at their disposal for carrying out these checks.

2.81 Given the clear risk posed by known bad actors, providers taking reasonable steps, including account checks, to prevent banned advertising account holders from advertising on the service would deliver significant benefits.

Checks for accounts with a risk that they will post fraudulent advertising, so that restrictions can be applied to them

2.82 By identifying indicators that there is a material risk an account will post fraudulent advertising through the fraud indicator assessment, providers would be better able to find accounts with these indicators. Where providers subsequently place a restriction on these accounts, they would reduce the risk of these accounts exposing large volumes of users to fraudulent advertising. We know these are currently used by providers, for example, Google's 'limited ad serving policy'.[46]

2.83 Placing restrictions on accounts which providers suspect belong to previously banned advertising account holders will give additional protections for users. While the provider cannot determine the account holder has been previously banned and so needs to be prevented from being able to advertise altogether, these accounts still pose a risk of posting fraudulent advertising.

2.84 We consider that each of the types of restriction we set out in paragraph 2.45 is likely to prevent users encountering fraudulent advertising because:

- Restrictions that limit the spend or the number of users who are able to encounter an advert will reduce the number of UK users who can see it.[47]
- Restrictions on targeting users from particular groups would limit the ability of the accounts to heavily target groups which may be particularly vulnerable to fraudulent advertising they post. Granular targeting is offered on services, and this could be exploited to reach vulnerable groups.[48]
- Restrictions to the advertising formats an account can use can also reduce the ability of bad actors to cause harm. For example, not allowing an account to post video advertisements (a restriction to formats) would reduce risk where there are indicators

[44] Signatories of the Home Office fraud charter agreed to "Explore what data, both internal and external, could facilitate the identification and prevention of fraud". Source: Home Office, 2023. Online Fraud Charter. [accessed 11 May 2026].
[45] The Global Signal Exchange has "deliberately chosen the term 'signal' to describe the information shared within it". Signals are an "indication of potential concern". Source: Global Signal Exchange, 2025. What is a Signal? [accessed 10 June 2026].
[46] Google, no date. Limited ad serving. [accessed 24 March 2026].
[47] Evidence from the Integrity Institute notes limiting the amount of advertisements an advertising account holder can post is an action platforms can take, and that 'limiting posting' is a relatively high-impact intervention. Source: Ofcom and Integrity Institute, 2026. Fraudulent advertising and account integrity: Expert insights on best practice.
[48] Ofcom, 2026. Behavioural audit of services with advertisement functionality.

the account might use video advertising to disguise the intention of their advertising, and make fraudulent advertising harder to detect and moderate.

- Moderating an account's content before it can go live means a service provider can identify fraudulent advertising and take appropriate action before users are able to encounter it.

2.85 We therefore consider that this part of the proposed measure will be effective at placing restrictions on accounts where there is an increased risk of harm, therefore limiting the opportunity for those accounts to potentially disseminate fraudulent advertising to users.

2.86 The benefits of this aspect of the proposed measure are further strengthened by its flexible structure, which allows providers to carry out a broad range of checks to suit the needs of their services. The checks providers do could include checks against public registers or business registration records. Providers can gather information on the registers and datasets that are available and design such checks according to the sources and accounts they intend to allow advertising from. As fraud is inherently adversarial and tactics vary between services, providers need to take a service-specific approach to finding accounts with indicators that there is a material risk they will post fraudulent advertising.

2.87 Providers are expected to update their fraud indicator assessment at least every 12 months.[49] Providers will need to update the checks they do as needed to take into account the most recent assessment. This means the checks providers do should also evolve to remain effective over time.

2.88 We also expect providers to keep a record of the restrictions they place on accounts. This will ensure providers can effectively monitor outcomes over time and update their policy to ensure restrictions are effective. We set out in Volume 1, Section 5, 'Approach to codes', sub-section 'Approach to record-keeping' the wider benefits of record-keeping.

The role of identity verification using ID documents in account checks

2.89 As highlighted in the sub-section 'Explanation of the measure', a way providers could comply with parts of the measure could involve identity verification using ID documents (for example, passport or driving licence). We are aware that some providers already do this in certain circumstances under their existing policies.[50]

2.90 Our proposed measure is designed to be flexible about how providers use identity verification with ID documents in the design of their checks, provided they align with our expectations. This is because the methods available to providers to carry out identity verification are likely to change over time. New methods could be more effective at meeting the aim of the recommendations or could reduce the impacts on providers or advertising account holders.

---

[49] See Volume 2, Section 3, 'Fraud indicator assessment', subsection 'Reviewing the assessment and tracking new indicators of fraudulent advertising'.

[50] X use identity verification for political advertisements certifications. Source: X, 2025. ID Verification Policy and Privacy. [accessed 27 May 2026]; Meta set out that "If the advertiser or payer of the ad is a person, they will need to complete verification using their government-issued ID". Source: Meta, 2026. About advertiser verification for ads transparency. [accessed 11 May 2025]; Google describe how identity verification using documents is used for reasons including building trust in advertisements. Source: Google Advertising Policies Help, 2026. Document requirements for advertiser verification. [accessed 27 May 2026]; Microsoft describe how, in order to "verify as an individual" under their verification process, individuals need to "provide documentation to verify your personal identity". Source: Microsoft, no date. Advertiser identity verification. [accessed 27 May 2026].

2.91 One reason for changes in methods available could be the UK Government's approach to identity verification. For example, the UK Government introduced proposals, in late 2025, for a GOV.UK Wallet and app which will allow for digital driver's licences, as well as a new voluntary digital ID scheme proposed for UK citizens and legal residents.[51] It is also developing a statutory regulatory framework for digital verification services to ensure that people and businesses can access trusted and secure digital identities.[52]

2.92 We are also aware that providers may check or verify information about users for a range of different reasons or purposes, including to meet various duties.[53]

Benefits of the steps to develop, review and update the policy we are proposing

2.93 Bad actor tactics change over time so providers should periodically update their policies to make sure they remain effective. We understand that information made available from internal and external experts in fraud, including reports from trusted flaggers, is likely to be particularly valuable in identifying emerging trends in fraud.[54] Trusted flaggers have particular expertise, so will likely provide valuable information regarding the prevalence of fraud on services and the role account checks can play to reduce it. Using these to develop and review the policy would therefore ensure that the policy is responding to new and adversarial fraud tactics.

2.94 We consider that 'at least every 12 months or if there is a significant change in the way advertising on the service operates' is an appropriate time period for frequency of review and update of the policy. This is for the same reasons this has been used in the proposed fraud indicator assessment measure.[55] Fraudulent advertising evolves rapidly, and there are clear costs to relying on outdated tactics rather than adopting new and effective checks as they emerge. Both proposed measures reflect the need for providers to adapt their systems to adversarial behaviour, and our intention to align review cycles with governance activities where possible.

2.95 We also think there are benefits to providers keeping a record of their reviews and superseded account checks and actions policies. We think this will support effective governance around account checks and actions, leading to providers being more effectively able to improve their approach over time. This is in addition to other benefits of record-keeping as set out in Volume 1, Section 5, 'Approach to codes', sub-section 'Approach to record-keeping'.

---

[51] GOV.UK, 2025. Digital driving licence coming this year. [accessed 17 June 2026]; GOV.UK, 2026. Digital ID scheme: explainer. [accessed 18 June 2026].

[52] GOV.UK, 2025. UK Digital identity legislation passes another important milestone. [accessed 17 June 2026].

[53] We note that Category 1 providers will also be in scope of the user identify verification duties set out in sections 64 and 65 of the Act. We are consulting separately on our proposals for guidance on how to comply with these duties (see 2026 Additional Duties Consultation). The fraudulent advertising duties are separate to the identity verification duties. It is for providers to ensure that their systems and processes are sufficient to comply with the user identify verification duties, where applicable.

[54] For example, the National Economic Crime Centre (NECC) publish an annual report on economic crime. Source: NECC, 2025. National Economic Crime Centre Annual Report 2024-25. [accessed 19 May 2026].

[55] See Volume 2, Section 3, 'Fraud indicator assessment', subsection 'Benefits and effectiveness of reviewing the assessment and tracking new indicators'.

Impacts and costs on service providers

2.96 This sub-section considers the main potential impacts and costs associated with our proposed measure for service providers, and advertising account holders.

Direct costs for service providers

2.97 Firstly, we consider how service providers could implement the proposed measure and seek to estimate the respective costs where possible for its main components.

2.98 In estimating costs, we assume that service providers will incur the costs of implementing an account checks and actions policy for the first time. However, in practice, providers are already likely to have some of the relevant systems and processes needed to carry out account checks and actions. We expect they could use and build on these systems and processes to align with our proposed measure for a lower cost than setting up a policy from scratch.

2.99 We expect costs to vary widely across individual service providers. This is due to factors such as the outcome of their fraud indicator assessment (for example, number of indicators of fraudulent advertising identified on their service), the range of account checks and actions they implement, the number of new accounts on a service each year, and their unique internal processes, which we note that our cost estimates cannot fully account for.

Having and applying an account checks and actions policy (one-off costs)

2.100 We expect service providers would need to dedicate staff time towards developing a policy on the account checks and actions they carry out. This would involve reviewing findings from the fraud indicator assessment as well as other sources of information, determining the relevant checks and actions to apply and when, writing an overall policy explaining these checks and actions, and obtaining sign-off on the policy from senior management.[56] We expect there would also be some further work associated with writing and approving a high-level summary of the policy and publishing this.

2.101 We assume this could require a team consisting of two professional occupation staff (for example, a policy manager and a legal employee) for three months to develop and draft the overall policy, with input from one software engineer and one content moderator for one month, and one day of a senior director's time to review and approve the policy, including the high-level summary that would be published. We estimate this could cost providers around £37,700 to £74,500.[57] However, these costs are likely to depend on the complexity and detail in the policy, as well as providers' internal processes for developing and approving new policies, and therefore costs could be higher for some providers.

2.102 To ensure the policy is consistently applied, we expect service providers would then need to dedicate staff time and resources towards communicating the detail of the policy and providing training to relevant individuals working on checking new accounts, so that they

[56] We expect the costs of providers undertaking the fraud indicator assessment and using it to understand the indicators of fraudulent advertising that exists on their services would be captured as part of the proposed fraud indicator assessment measure. See Volume 2, Section 3, 'Fraud indicator assessment', subsection 'Impacts and costs on service providers.'

[57] Based on our labour wage assumptions as set out in Annex 8, 'Further detail on economic assumptions and analysis'.

understand how to implement it. We estimate it could cost providers around £190 to £390 to train each individual working on checking new accounts in line with the policy.[58]

Specific account checks and actions the policy should include (one-off and ongoing costs)

Verification that advertising account holders work for or on behalf of the individual or organisation being advertised

2.103 Our proposed measure expects providers to first understand the relationship that the person setting up the account has with the individual or organisation they are advertising. We outlined some methods that could be used to do this in paragraph 2.20, which are likely to have different costs. These costs will vary depending on the method and whether a service already uses similar approaches. In general, providers will have the flexibility to choose the method or combination of methods most cost-effective for them.

2.104 Our proposed measure then expects providers to verify that the advertising account holder does work for, or on behalf of, the individual or organisation they will advertise. Providers will have the flexibility to decide whether to undertake the check in-house or using a third-party provider, and the specific method of verification. We are aware that some service providers outsource parts of their account checks to third-party suppliers.[59] Outsourcing these checks to third-party suppliers could represent a lower set-up cost option for some providers, relative to building a verification system in-house to undertake these checks.

2.105 We consider in the following paragraphs the costs to service providers of using a third-party supplier to verify if advertising account holders can demonstrate ownership of contact details (for example, email or phone number) linked to the individual or organisation being advertised.

2.106 There are likely to be one-off set-up costs associated with onboarding and integrating a third-party supplier. We consider these would mainly be staff costs. We assume providers may need around three to six months with input from one software engineer, one IT project manager and one other professional occupation staff member, tasked with procuring the third-party supplier, onboarding them, and integrating the relevant application programming interface (APIs). Using our standard wage assumptions, we estimate the provider would incur one-off set-up costs in the range of £48,300 to £193,000.[60] In general, we expect costs to vary across providers based on their internal processes for onboarding new suppliers and the technical complexity of their service.[61]

2.107 The potential ongoing costs of using a third-party supplier are likely to scale with the number of accounts that need to be verified each year. These costs are likely to include annual licensing costs and the costs per verification undertaken, as well as any ongoing maintenance costs. Most suppliers of one-time passcode authentication solutions operate a pay-as-you-go pricing model, which means that providers only pay for the number of verifications undertaken. Based on publicly available price points, we observe that suppliers

[58] We assume it takes one day to train an individual, and estimate costs based on the salary of a content moderator. See Annex 8 'Further detail on economic assumptions and analysis' for more details.
[59] [✂] response to our formal information request issued 30 January 2026; [✂] response to our formal information request issued 30 January 2026.
[60] Based on our labour cost assumptions as set out in Annex 8, 'Further detail on economic assumptions and analysis'.
[61] For example, we expect integrating a third-party supplier could be more challenging for services with a large number of relevant functionalities.

charge around £0.04 per successful email verification and £0.05 per successful SMS verification.[62] Therefore, we expect that a provider onboarding around 400,000 new advertising accounts per year[63] would incur costs ranging from £16,000 to £20,000 to verify account holders' contact details. Some suppliers offer volume-based discounts, which could help lower the cost per verification.[64] We also expect providers to incur ongoing maintenance costs of between £12,100 and £48,300 per year associated with maintaining integration with the APIs and applying updates where needed.[65]

Checks that providers carry out to prevent banned advertising account holders returning

2.108 There would be one-off and ongoing costs associated with implementing checks to determine whether an advertising account holder was previously banned. At a minimum, we expect that providers would need to incur costs associated with collecting the relevant information from new advertising account holders, and checking this information against information held about advertising account holders of banned accounts (see paragraph 2.26).

2.109 We are aware that many Category 1 and 2A services already collect information such as the name, email address and phone number of the advertising account holder.[66] We expect any additional costs of implementing and maintaining the systems and processes that can be used to collect this information from new advertising account holders is therefore likely to be low. Cross-referencing this information against information held on holders of banned advertising accounts would involve providers storing relevant information about banned advertising account holders, processing this information to produce a searchable database, and implementing a system to cross-check against this database and return the nearest possible matches. We assume this could require input from one software engineer for three months and one IT project manager for one month. Based on this, we estimate there could be one-off costs to providers of around £22,800 to £45,600 to process the relevant information and implement the necessary systems, and ongoing costs of around £5,700 to £11,400 per year associated with maintaining the systems.[67]

Checks for accounts with indicators that there is a material risk they will post fraudulent advertising

---

[62] SMS pricing typically depends on the destination of the message being sent. This pricing assumes the SMS is sent and received in the UK. Twilio, no date. Transparent, scalable, usage-based pricing for Twilio SMS and RCS. [accessed 30 April 2026].

[63] We have estimated this figure based on the average number of distinct advertising accounts onboarded in 2024/25 by six providers. Sources: [✂] response to our formal information request issued 30 January 2026; [✂] response to our formal information request issued 30 January 2026; [✂] response to our formal information request issued 30 January 2026; [✂] response to our formal information request issued 30 January 2026; [✂] response to our formal information request issued 30 January 2026; [✂] response to our formal information request issued 30 January 2026.

[64] Twilio. Transparent, scalable, usage-based pricing for Twilio SMS and RCS. [accessed 30 April 2026]. See footnote 62 for more information.

[65] Our standard assumptions are that maintenance would be 25% of the initial set-up costs. See Annex 8 'Further detail on economic assumptions and analysis' for more details.

[66] Sources: Google response to our formal information request issued 26 June 2025; [✂] response to our formal information request issued 26 June 2025]; Microsoft response to our formal information request issued 26 June 2025; [✂] response to our formal information request issued 26 June 2025.

[67] Consistent with our standard assumptions as set out in Annex 8 'Further detail on economic assumptions and analysis', we assume that the ongoing maintenance costs are 25% of the initial one-off set-up costs.

2.110 There would also be one-off and ongoing costs associated with implementing the checks to determine whether an account presents specific indicators of fraudulent advertising and applying restrictions if needed.

2.111 We expect that the costs would vary widely across services, based on the type and number of fraudulent advertising indicators a provider identifies, and the extent to which a provider would subsequently have to tailor their onboarding process to identify these indicators and apply restrictions. Due to the diverse range of services involved and checks and restrictions that could be implemented, it is challenging to estimate the potential costs service providers could incur. However, at a high level, we expect providers would incur one-off costs in relation to development, testing and production of their systems and processes used to undertake the checks and apply the restrictions, as well as ongoing costs in the form of record-keeping, monitoring and maintenance.

Development, regular review and update of the account checks and actions policy (ongoing costs)

2.112 To initially develop as well as review and update the policy at least every year, we expect that service providers, at a minimum, would need to examine findings from the fraud indicator assessment, information made available by experts in fraud including trusted flagger reports, and previous advertisement moderation decisions. To review and update their policy over time, we expect providers to additionally consider whether there have been any changes to the nature and functionality of their service and changes to technology and tactics that can be used by fraudsters and providers (see paragraph 2.55).

2.113 We have considered the costs of initially developing the policy in the sub-section 'Having and applying an account checks and actions policy (one-off costs)'. For the regular review and update of the policy, we assume this could require a small team consisting of a mix of professional occupation staff (for example, a policy manager and a lawyer), content moderators and software engineers, and could cost providers around £10,200 to £20,300 each year.[68] Providers could also rely on data-driven modelling (such as machine-learning models) to examine and review relevant findings, which could involve higher costs associated with data collection, preparation, model development and training, but could help reduce ongoing staff resources and costs.

2.114 We expect any updates would need to be written down and approved. We estimate this could cost service providers between £4,100 and £7,700 per year, in addition to costs associated with communicating the updates to all relevant individuals working on checking accounts.[69] In practice though, these costs will depend on the number and extent of updates made per year, and the internal processes of providers for approving policy changes.

Total costs

[68] This estimate is based on providers needing two weeks of time from two professional occupations staff members and two content moderation staff members, and one week of time from a software engineer.
[69] We assume it could require three weeks of input from a professional occupation staff member (for example, policy manager, lawyer) to draft updates to the policy and half a day of input from a senior director to review and approve these updates.

2.115 As summarised in Table 2.1, we have been able to estimate one-off costs of around £109,000 to £313,000 and ongoing costs of around £48,000 to £108,000 per year.[70] [71] However, we have only been able to qualitatively consider other costs, due to the wide variation in the range and type of checks and restrictions that service providers could implement. Therefore, our total estimated costs for a service provider implementing an account checks and actions policy for the first time is likely to be an underestimation.

Table 2.1: Summary of estimated one-off and ongoing costs per year

Measure component	One-off costs	Ongoing costs (per year)
Having and applying the policy	£37,700 to £74,500	Not applicable
Verification that the advertising account holder is working for the individual or organisation they advertise	£48,300 to £193,200	£28,100 to £68,300
Checks to prevent banned advertising account holders returning	£22,800 to £45,600	£5,700 to £11,400
Checks for accounts with indicators that there is a material risk that they will post fraudulent advertising, so that restrictions can be applied to them	Not quantified	Not quantified
Development, regular review and update of the policy	Not applicable	£14,300 to £28,000
Total estimated costs	£109,000 to £313,000	£48,000 to £108,00

2.116 Many Category 1 and 2A services already carry out account checks and apply restrictions to accounts that violate their advertising policies. We expect they could utilise and build on

[70] The total one-off costs consist of the costs associated with providers developing, drafting and approving an account checks and actions policy; onboarding and integrating a third-party supplier to verify if advertising account holders can demonstrate ownership of contact details linked to the organisation or individual being advertised; and implementing a system to cross-reference information obtained on new advertising account holders against that held on holders of banned advertising accounts. It does not include the potential one-off costs associated with providing training to relevant staff on the overall policy, or the one-off costs associated with implementing checks and restrictions for accounts with indicators of fraudulent advertising.

[71] The total ongoing costs consist of the costs associated with verifying the contact details of 400,000 new advertising accounts each year, the annual costs of maintaining the systems used for this verification as well as the systems used for checking for account holders of banned advertising accounts, and the costs associated with the regular review and update of the overall account checks and actions policy. It does not include the potential ongoing costs associated with having checks and restrictions for accounts with indicators of fraudulent advertising, or the ongoing cost of training on the account checks and actions policy.

these systems and processes to reduce costs.[72] [73] We have designed the proposed measure to be flexible so that providers can introduce it in the most cost-effective way for them.

2.117 We further note that there could be some overlap in costs between this proposed measure and our proposed financial services verification and proposed countering account takeover measures.[74] Service providers could choose to adopt verification systems or methods (for example, one-time passcodes) that could effectively be used across a range of checks we are proposing, therefore saving costs.

Indirect costs to service providers

2.118 Our proposed account checks could deter legitimate advertisers from advertising in a number of ways:

a) if the checks are perceived to be too complicated so advertisers decide not to complete them,
b) if legitimate advertisers fail the checks

In turn, this could lead to a loss of advertisements and therefore revenues for Category 1 and 2A services.

2.119 We expect this risk to overall be very low. Category 1 and 2A services can target adverts at a lot of users which means they likely to be highly attractive to advertisers. Therefore, the risk advertisers may all together be deterred from advertising on these services is likely to be low. We also expect that providers will have strong incentives to ensure that the checks are as straightforward as possible and that support is available to legitimate advertisers that may fail to achieve the necessary verification at first instance.

Impact on advertising account holders

2.120 The proposed different account checks could increase the time as well as resources needed for legitimate advertising account holders to complete the relevant account checks before they can start placing advertisements.

2.121 However, service providers will have the incentives to ensure that the additional checks are as quick and easy to complete as possible. We consider the account checks would be effective at finding and restricting accounts with indicators that there is a material risk they will post fraudulent advertising, hence protecting users from harm over time. In the longer

---

[72] For example, verifying contact details using one-time passcodes, checking information from third-party sources, and scanning for signs of compromised payment cards. Sources: [✂] response to our formal information request issued 26 June 2025; [✂] response to our formal information request issued 26 June 2025; [✂] response to our formal information request issued 26 June 2025; [✂] response to our formal information request issued 26 June 2025; [✂] response to our formal information request issued 26 June 2025.

[73] For example, Microsoft allows up to three strikes for advertising policy violations before suspending advertising accounts. Source: Microsoft, 2025. What happens when an Ad policy is violated. [accessed 7 April 2026]; We are aware that Meta has an account integrity policy that details the circumstances under which Meta may restrict or disable advertising accounts. Source: Meta, 2026. Account integrity. [accessed 7 April 2026]; Google sends a warning and applies a maximum of three strikes on accounts if found to have violated their advertising policies, with the third strike resulting in account suspension. Source: Google, no date. Google Ads account suspensions overview. [accessed 7 April 2026].

[74] See Volume 3, Section 3, 'Preventing fraudulent financial services advertising' and Volume 3, Section 4, 'Countering account takeover'.

term, this could lead to greater user trust and engagement with legitimate advertisements and so benefit advertising account holders.

2.122 We are also aware that there is the risk that some legitimate accounts, most likely smaller businesses that may not have the information or corporate assets required, or have limited time and resources to produce the information required, could fail the checks and fail to achieve the necessary verification as part of our proposed measure.[75] For example, they could submit incomplete or outdated information. This could lead to advertising account holders being unable to advertise on services or being subject to restrictions, which could have a negative impact on their potential sales and revenues. However, we consider this risk should be mitigated by our proposed measure on giving advertising account holders a means to appeal if they do not pass the checks at first instance, which we set out in Volume 3, Section 6, 'Account appeals'.

Other impacts

2.123 The additional frictions advertising account holders are expected to face because of the different checks proposed could lead to fraudsters seeking alternative ways to post fraudulent advertisements. We acknowledge there is a risk that our proposed measure could lead to fraudsters attempting to gain access and take over existing legitimate advertising accounts to post fraudulent advertisements, instead of setting up accounts from scratch. However, we expect this risk would be mitigated by our proposed countering account takeover measure set out in Volume 3, Section 4, 'Countering account takeover'.

Rights assessment

Freedom of expression

2.124 As explained in Volume 1, Section 5, 'Approach to codes', subsection 'Approach to human rights assessments', Article 10 of the European Convention on Human Rights (ECHR) protects the right to freedom of expression, including the freedom to hold opinions and to receive and impart information and ideas without interference by a public authority. Article 10 is a qualified right, and we must exercise our duties under the Online Safety Act 2023 (the Act) in a way that does not restrict this unless satisfied that it is proportionate to the legitimate aim pursued. As noted within 'Approach to codes', we start from the position that these proposed measures are prescribed by law, are in pursuit of a legitimate aim and correspond to a pressing social need.

2.125 The proposed account checks measure has the potential to impact on the freedom of expression rights of users, advertisers and providers of Category 1 and 2A services. We have focussed on the potential impact on the freedom of expression rights of users and advertisers, to the extent that they use the service to communicate commercial messages, as we consider this is likely to be more significant.

2.126 We recognise that interference with advertising account holders' rights to freedom of expression may arise as a result of the proposed measure, which may lead to advertising account holders being unable to create an account or alternatively where they are prevented from being able to advertise on the service, or have restrictions placed on their advertising functions.

[75] For example, the company the advertising account holder works for may not have a cooperate email address or it could be a sole trader, and so not appear on lists of registered companies.

2.127 Further, such interference may be more acute in circumstances where the account checks carried out by providers result in inaccurate judgements being made, for example, an account being erroneously noted as having an indicator that there is a material risk it will post fraudulent advertising or is erroneously suspected of belonging to a banned person, leading to legitimate advertising accounts being prevented from placing advertisements on the service, or having restrictions placed on their advertising functions. We recognise that some providers may choose to set a more stringent policy, to ensure it is clear that they are following the recommendations in this proposed measure, which may further impact genuine advertising account holders' freedom to post advertising content and potentially limit or prevent their access to the service by not being permitted to create an account. In some cases, this may dissuade potential advertising account holders, including those who would have gone on to post legitimate advertisements, from advertising on services perceived to be carrying out stringent account checks. This would limit not only advertising account holders' rights to freedom of expression to freely impart ideas but also prevent users from being able to receive information and ideas from paid-for advertisements which should not have been prevented from being placed on the service.

2.128 Our proposed measure on account appeals (see Volume 3, Section 6, 'Account appeals') acts as a safeguard for freedom of expression. This proposed measure allows advertisers to appeal against decisions taken by service providers following failed account checks and to provide additional information to providers, who may overturn any action taken in response to an appeal.

2.129 Providers are expected to use findings from the proposed fraud indicator assessment to determine which accounts have indicators suggesting that there is a material risk they will post fraudulent advertising, and place restrictions on them. The rights impacts of the fraud indicator assessment are set out in Volume 2, Section 3, 'Fraud indicator assessment', sub-section 'Rights Assessment'.

2.130 We also recognise that this proposed measure may engage providers' rights to freedom of expression, as they potentially could limit who providers can allow to advertise on their service, and also impact providers' autonomy and how advertising content is communicated.

2.131 We consider that implementing the proposed measure is important in enabling service providers to meet their fraudulent advertising duties under the Act. The proposed measure is designed with proportionality in mind, given the proposed flexible approach, and is also intended to be the least intrusive means to ensure that an effective assessment is made to identify accounts that are likely to be operated by bad actors, and mitigate associated risks. As noted in 'Benefits and Effectiveness', we consider that the proposed measure helps address the significant harm caused by fraudulent advertising.

2.132 Overall, to the extent that this proposed measure involves interference with individuals' and advertisers' rights to freedom of expression, we consider the interference to be proportionate to the Act's legitimate objective of protecting individuals in the UK from fraudulent advertising (which this proposed measure is intended to help providers of Category 1 and 2A services to secure).

Data protection and privacy

2.133 As explained in Volume 1, Section 5, 'Approach to codes', subsection 'Approach to human rights assessments', Article 8 of the ECHR confers the right to respect for an individual's private and family life. Article 8 is a qualified right, and we must exercise our duties under

the Act in a way that does not restrict this right unless satisfied that is proportionate to the legitimate aim pursued. Again, we start from the position that this proposed measure is prescribed by law, in pursuit of a legitimate aim and corresponds to a pressing social need. Article 8 underpins the data protection laws with which service providers must comply.

2.134 We recognise that interference with advertising account holders' rights to privacy may arise where account checks are being carried out as a result of the proposed measure, in particular, checks to understand the relationship with the organisation or individual the advertising account holder will be advertising and verification that advertising account holders do work for or on behalf of that organisation or individual, to prevent banned advertising account holders from returning or due to the presence of particular indicators suggesting that there is a material risk they will post fraudulent advertising. This is likely to arise when the advertising account holder first sets up an account on the service, and where any further checks are conducted as a result of changes to relevant information relating to the account.

2.135 We consider that, depending on the systems and processes used by service providers, the proposed account checks measure is likely to involve processing advertisers' personal data at scale and also potentially the processing of special category data. The UK General Data Protection Regulation (GDPR) places a specific restriction on making decisions based solely on automated processing of personal data, where the decision has legal or similarly significant effects. These restrictions are imposed by Articles 22A to D of the UK GDPR.[76] So-called automated decision-making is permitted where service providers have appropriate safeguards in place. Additional restrictions also apply in relation to cases where special category data is used. The Information Commissioner's Office (ICO) has provided guidance on these matters.[77]

2.136 Service providers should ensure they, or any third parties that they outsource to, act in accordance with data protection legislation and relevant ICO guidance and consider the data protection principles of fairness, transparency and data minimisation in implementing this proposed measure.[78] Providers will also need to ensure that data protection impacts are limited to what is necessary for the legitimate purpose of complying with the fraudulent advertising duties. We consider that safeguards under data protection law, as explained in the various pieces of ICO guidance, will help ensure that the impact of processing (including automated processing) on data protection and privacy rights is minimised.

2.137 To the extent that this proposed measure involves interference with individuals' rights to privacy, we consider the interference to be proportionate to the Act's legitimate objective

---

[76] Articles 22A to D were substituted for Article 22 by section 80(1) of the Data (Use and Access) Act 2025, with effect from 5 February 2026: see the Data (Use and Access) Act 2025 (Commencement No. 6 and Transitional and Saving Provisions) Regulations 2026, regulation 2(j), subject to regulation 5.

[77] See ICO, no date. UK GDPR guidance and resources; In the context of these proposed measures, in some instances this may involve 'storage and access technologies' which engage the requirements set out in Regulation 6 of the Privacy and Electronic Communications Regulations. The ICO has also provided guidance on this matter. See ICO, 2026. Guidance on the use of storage and access technologies. [accessed 22 May 2026].

[78] See ICO, no date. UK GDPR guidance and resources; In the context of these proposed measures, in some instances this may involve 'storage and access technologies' which engage the requirements set out in Regulation 6 of the Privacy and Electronic Communications Regulations. The ICO has also provided guidance on this matter. See ICO, 2026. Guidance on the use of storage and access technologies. [accessed 22 May 2026].

of protecting individuals in the UK from fraudulent advertising (which this proposed measure is intended to help providers of Category 1 and 2A services to secure).

Provisional conclusion

2.138 All Category 1 and 2A service providers must have in place proportionate systems and processes designed to protect users from fraudulent advertising in accordance with their duties under sections 38(1) and 39(1) of the Act. Our proposed approach is to recommend service providers have and apply an account checks and actions policy as a preventative step to protect users from encountering fraudulent advertising.

2.139 For the reasons we have set out, we provisionally consider that the proposed checks would be effective at combatting fraudulent advertising and would deliver material benefits.

2.140 We expect that the proposed measure could result in significant costs for providers, and material impacts on the rights of advertising account holders. However, our provisional view is that these impacts would be proportionate given the significant scale of the harm fraudulent advertising causes and the role this measure could play in addressing it.

2.141 Our provisional view is therefore that it is proportionate to recommend that Category 1 and Category 2A services have and apply an account checks and action policy and carry out the checks we propose.

2.142 The full text of the proposed measure can be found in the draft Fraudulent Advertising Code of Practice for user-to-user services and in the draft Fraudulent Advertising Code of Practice for search services, and they are referred to as FAU H1 and FAS H1 respectively.

3. Preventing fraudulent financial services advertising

What is this section about?

This section sets out the steps we propose service providers should take to ensure that individuals and firms can only advertise financial services products where they have the relevant legal permissions to do so.

It sets out our proposed measure on financial services verification for service providers, and why we are recommending it.

Our proposal

Number in our Codes	Proposed measure applicable to providers of Category 1 and 2A services
FAU H2 and FAS H2	Providers should **have and consistently apply a financial services verification policy**. It should set out: the types of financial services advertising allowed as well as prohibited on the service; how the provider will **find financial services advertisements** and those posting them; and how the provider will **verify** that individuals and firms posting financial services advertising have **the appropriate legal permissions before advertisements are able to be encountered by UK users**. Providers should also publish a summary of this policy and review and update their policy at least every 12 months.

Why are we proposing this?

Fraudulent financial services advertising causes significant harm. In the UK, financial services advertising targeting UK consumers can only be issued or approved by individuals or firms authorised by the Financial Conduct Authority, unless an exemption applies. We are proposing that service providers check that any individual or firm wishing to advertise financial products and services is legally permitted to do so. The available evidence suggests that this will significantly reduce the amount of fraudulent advertisements for financial services products that users are exposed to.

Consultation question

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

Introduction

3.1 Fraudulent financial services advertising causes significant harm to users, including high-value harm arising from investment fraud.[79] While advertising systems play an important role in enabling legitimate businesses and individuals to promote financial services, they may also be exploited by bad actors promoting financial services unlawfully to defraud users.

[79] We have set out the meaning of the term 'financial services advertising' within Annex 7, 'Glossary', and in paragraph 3.9 below. For more information regarding the harm from investment fraud, see Volume 1, Section 4, 'Causes and impacts of fraudulent advertising', paragraph 4.23.

3.2 In the UK, financial services legislation places important restrictions on the promotion of financial products and services. It is a criminal offence to communicate a financial promotion unless it is issued or approved by a firm authorised by the Financial Conduct Authority (FCA), or where an exemption applies in limited cases. [80] [81] [82]

3.3 In this section, we propose that providers put in place verification checks and actions designed to ensure that anyone advertising financial services has the appropriate permissions before advertisements are able to be encountered by UK users.[83]

3.4 By reducing the amount of financial services advertising posted by those not legally permitted to advertise such products, this proposed measure should materially reduce the risk of users being exposed to online financial fraud.

3.5 In this section, we outline and examine our proposals in detail. We explain how and when we consider financial services verification should be applied, the benefits and effectiveness of applying it and the impacts.

3.6 We acknowledge that a Category 1 or 2A service may be serving paid-for advertisements to its users through different advertising pathways. Where relevant, the proposed advertising intermediaries measure would apply. The proposed advertising intermediaries measure recommends that a provider should use all reasonable endeavours to implement a version of any measures it has been unable to apply. For more information, see Volume 2, Section 2, 'Advertising intermediaries.'

---

[80] The FCA authorises and supervises firms that carry out regulated financial activities, such as advising on, arranging or offering certain financial products and services, to help ensure that markets work properly and that consumers are appropriately protected. Source: FCA, 2026. About the FCA. [accessed 30 June 2026].

[81] Where advertising seeks to persuade or incite a person to engage in a regulated financial activity as defined in applicable financial services legislation (such as activities that are controlled financial services activities in the UK and are set out in Schedule 1 to the Financial Services and Markets Act 2000 (Financial Promotion) Order 2005),, this type of advertising in the UK will generally be subject to the communication restrictions under section 21 of the Financial Services and Markets Act 2000 (FSMA) – known as the 'general restriction'. It is a criminal offence under section 25 of FSMA to communicate financial promotions where these are not issued or approved by a firm authorised by the FCA, unless the promotion is otherwise exempted. Exemptions are primarily set out in the Financial Promotion Order 2005 (FPO); From our engagement with the FCA, we understand that the applicability of exemptions online is likely to be highly limited. Many exemptions in the FPO (such as the High Net Worth or Sophisticated Investor exemptions), are subject to strict criteria being met and rely on advertisers being able to segment the customers they are aiming to reach to a degree of specificity not possible on mass-reach services. Source: FCA written response dated 3 March 2025 to Ofcom engagement on 17 February.
Contraventions of the general prohibition under section 25 of FSMA are a fraud offence listed in section 40 of the Online Safety Act 2023.

[82] The FCA has published guidance on the definitions and rules applicable to the promotion of financial services and products. Sources: FCA, 2024. Financial Promotions and adverts. [accessed 30 June 2026]; FCA, 2024. FG24/1 Finalised Guidance on Financial Promotions on Social Media. [accessed 30 June 2026]; FCA, 2026. PERG 8: Financial promotion and related activities. [accessed 30 June 2026].

[83] Verification is the process of checking that something is true and accurate, using specific evidence to confirm this.

Financial services verification

Explanation of the measure

3.7 We propose that service providers should adopt and consistently apply a financial services verification policy designed to prevent individuals and firms who are not legally permitted to advertise financial services to UK users from doing so on their service.

3.8 Financial services verification should take place before paid-for financial services advertisements are able to be encountered by UK users. This includes verification of all new and existing advertising accounts on the service seeking to post financial services advertising.

3.9 As set out in Annex 7, 'Glossary', we consider that financial services advertising means any paid-for advertising that promotes, or is capable of promoting, financial products or services. This includes advertising for common types of financial services and products, including, but not limited to, investments, credit and loans, insurance, pensions, debt advice, and qualifying cryptoassets.

3.10 Providers should set out the following in their financial services verification policy:

a) The types of financial services advertising they allow, who is allowed to advertise them, and any types of financial services advertising they do not allow on their service.
b) How they will find financial services advertisements and the firms and individuals posting them.
c) How they will verify individuals and firms posting financial services advertising have appropriate legal permissions to do so. This should include at a minimum verifying whether individuals and firms promoting financial services are authorised by the FCA, the UK's regulator for financial services, and listed on the FCA Financial Services Register; and appear on the FCA Warning List as the subject of an alert.[84]

3.11 We set out our expectations for each of these components in paragraphs 3.13 to 3.40, under the heading 'What the financial services verification policy should include'.

3.12 Figure 3.1 provides a visual overview of how the proposed measure would work for providers that allow financial services advertising.

[84] The FCA Financial Services Register provides publicly available authoritative information on the firms and individuals that are authorised by the FCA to offer financial products and services in the UK. Source: FCA, 2026. Financial Services Register. [accessed 30 June 2026]; The FCA Warning List identifies entities the FCA believes may be operating without authorisation and may be running scams or otherwise causing harm. Source: FCA, 2026. FCA Warning List of Unauthorised Firms. [accessed 30 June 2026].

Figure 3.1: Financial services verification policy

What the financial services verification policy should include

The types of financial services advertising allowed on the service

3.13 Service providers should specify within their financial services verification policy:

a) the types of financial services advertising that are permitted on their service;
b) the types of financial services advertising that are not permitted on their service; and
c) those individuals and firms who are allowed to advertise financial services on the service, subject to verification being passed.[85]

[85] For example, providers could set their policy to only allow individuals and firms authorised by the FCA to post financial services advertising or tailor their policy to allow other ways in which individuals or firms may legally advertise financial services (for instance, if the advertisement is approved by someone authorised by the FCA, or if an exemption applies).

3.14 Providers should ensure, through the design and application of their policy, that firms or individuals can only advertise financial services where the provider has verified that they have the appropriate permissions to do so under the law.

3.15 We propose to recommend that service providers publish a high-level summary of their financial services verification policy. This should include the types of financial services advertising they permit and who is able to advertise them, and any types of financial services advertising they prohibit. We recognise that publishing too much detail could assist bad actors by revealing how verification operates. We therefore expect providers to share information at a sufficiently high level, without disclosing details that could be misused.

How providers find financial services advertisements and the firms and individuals posting them

3.16 Providers should clearly explain in their policy how they will find financial services advertisements and the accounts seeking to post them before such advertisements are able to be encountered by UK users, so that it can be subjected to verification.

3.17 The proposed financial services verification measure will only work effectively when service providers are able to detect financial advertisements, and through these, the individuals and firms posting them that need to go through verification. To achieve this, we provisionally consider that providers will need to deploy proactive technology to detect financial services advertisements prior to them being made available to UK users. We expect this would mean that all advertisements would need to be subject to detection processes before being shown to UK users. Human review alone is not suitable because providers in scope of the proposed measure host millions of advertisements a year.

3.18 We therefore intend to consult on a measure recommending that providers of Category 1 and 2A services use proactive technology to identify financial services advertisements. We explain more about this under 'Consultation on use of proactive technology to find financial services advertising' in paragraph 3.55.

3.19 Providers may supplement their use of proactive technology to find financial services advertisers with other methods. For example, providers who allow financial services advertising could gather information at the account or advertisement creation stage using self-declaration, which can be a useful way to gather information from legitimate actors about their intention to engage in financial services advertising and verify their ability to do so before they seek to place any advertisements.[86]

3.20 Providers may also become aware of financial services advertising made by an account that has already been made available to users in cases where it has not been detected by proactive technology (for example, through trusted flagger reports), and should act on these in accordance with those proposed measures.[87]

[86] However, any self-declaration will be susceptible to misuse by bad actors who will be dishonest about their intentions. Therefore, we consider that providers cannot rely on self-declarations alone to effectively find financial services advertising but should use them only where they can be supplemented by advertisement detection tools able to detect undeclared financial services advertising.

[87] 'Trusted flagger reports' refer to reports made by trusted flaggers as defined in Volume 4, Section 4, 'Advertising complaints', subsection 'Dedicated reporting channels for trusted flaggers to report fraudulent advertisements'.

How providers will verify individuals and firms posting financial services advertisements

3.21 Providers that allow financial services advertising to UK users should explain in their policy the processes and actions they will take to verify that individuals and firms advertising financial services are legally permitted to do so.

3.22 Providers should verify the legal permissions of anyone seeking to post financial services advertising to UK users as soon as they become aware of their intent to do so, and before any such advertisements are able to be encountered by UK users.

3.23 We acknowledge that in practice providers may become aware of this at different points, for example, when an advertising account is set up, when an advertising campaign is created or uploaded for publication, or when financial services content has been detected using proactive technology.

3.24 If a provider finds a financial services advertisement from an account that has not been verified after it has become available to users, it should suspend the advertisement from being available to UK users while verification is being carried out.

3.25 To verify that the individual or firm is legally permitted under UK law to promote the advertised financial services, providers should at a minimum carry out checks for whether individuals and firms promoting such advertisements:

are authorised by the FCA, and listed on the Financial Services Register;
appear on the FCA Warning List as subject to an alert.

3.26 These could be carried out by humans, via automated technology, or a combination of both. In paragraphs 3.27 to 3.37, we set out the steps providers should take and provide illustrative examples of what this could involve in practice.

Verifying if the individual or firm is authorised by the FCA and listed in the Financial Services Register

3.27 Verifying that an individual or firm is authorised by the FCA involves two distinct steps:

a) checking whether the individual or firm seeking to promote financial services appears on the FCA Financial Services Register; and
b) establishing that the individual or firm seeking to post financial services advertising is the authorised entity listed on the FCA Financial Services Register.

3.28 Only where both steps have been completed should providers conclude that the individual or firm is a legitimate actor with the appropriate legal permissions to advertise financial services.

3.29 When verification for FCA authorisation has been successfully completed, the provider can allow the associated account to advertise financial services to users.

Example 3.1: Verifying if the individual or firm promoting financial services is FCA-authorised

Step 1

The provider collects relevant information from the advertiser, including:

1. name of individual or legal entity name and trading name(s);
2. FCA Firm Reference Number (FRN);
3. corporate email address;

4. phone number;
5. registered address; and
6. website.

Step 2

The provider checks the FCA Financial Services Register manually or via application programming interface (API) to confirm that:

1. the FRN exists; and

2. the FRN, legal entity name and other publicly available details on the Financial Services Register (for example, website, email domain or phone number) match the information provided by the advertiser to the service.

Step 3

The provider sends an email containing a unique verification code to an address at a domain consistent with the FCA-registered contact details, enabling the recipient to demonstrate access to an email address associated with a domain linked to the information on the FCA Register.

Step 4

Where there is a positive match across the Financial Services Register details and successful verification of ownership of contact details, the provider may confirm that the individual or firm is authorised by the FCA and allow them to place financial services advertisements.

Checking if the individual or firm appears on the FCA Warning List as subject to an alert

3.30 As part of their checks, providers should assess whether an individual or firm seeking to promote financial services is listed on the FCA Warning List. The Warning List identifies entities the FCA believes may be operating without authorisation and may be running scams or otherwise causing harm.[88]

3.31 This check may be carried out alongside, or following, verification of FCA authorisation.

3.32 Where an individual or firm is listed on the FCA Warning List, providers should prevent them from advertising financial services. Providers should set this out in their policy.

Example 3.2: Checking if the individual or firm promoting financial services is on the FCA Warning List

Step 1

The provider collects information, including:

1. name of individual or firm;
2. physical address;
3. email address;
4. phone number; and
5. website or landing page URL.

Step 2

[88] FCA, 2026. Financial Services Register. [accessed 30 June 2026].

The provider searches for whether there is an entry in the FCA Warning List (directly, or via returns obtained by searches on the Financial Services Register (API) matching any of those details.[89]

Step 3

If a matching Warning List entry is found, the provider should conclude that the advertiser is subject to an FCA warning and should not be allowed to place financial services advertisements. The account holder or operator can submit an appeal of this decision under the proposed Account appeals measure (see Volume 3, Section 6, 'Account appeals').

Completing verification on individuals and firms not authorised by the FCA and not on the Warning List

3.33 There may be circumstances where individuals or firms seeking to promote financial services do not appear on the Warning List but are also not authorised by the FCA. These individuals or firms may nevertheless be able to promote financial services legally, for example if:

- the promotion has been approved by an FCA-authorised firm;
- the promotion is for qualifying cryptoassets and the firm or individual is registered with the FCA;[90] or
- the promotion falls within a valid exemption under the Financial Services and Markets Act 2000 (Financial Promotion) Order 2005 (FPO).[91]

3.34 In most of these cases, including where a promotion is approved by an authorised firm, the permission to promote financial services will likely apply only to the specific advertisement. In such circumstances, providers should treat verification as applying to that advertisement only, rather than as a broader or ongoing approval of the individual or firm.

3.35 Service providers should set out in their financial services verification policy if they will allow financial services advertising where the individual and firm is not listed on the Financial Services Register as authorised by the FCA but may be advertising under the circumstances set out above in 3.33. Where service providers choose to allow such advertisements, they should put in place checks to verify that the individual or firm posting the advertisement is legally allowed to do so. Providers should clearly set out in their policy the checks they will carry out and the information they will require.

3.36 Relevant information for these checks may include:

- written evidence of approval from an FCA-authorised firm (including contact details for verification);

---

[89] Searches against the FCA Warning List will need to account for variations in names (for example, abbreviations, punctuation, or different company suffixes such as 'Ltd' and 'Limited'), as the name used by an advertiser may not exactly match the form recorded on the list.

[90] Promotions for ('qualifying') cryptoassets are currently within scope of the FSMA and the FCA's remit. Individuals and firms may only promote cryptoassets where they are registered with the FCA under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs), they are already an authorised firm, their promotion has been approved by an authorised firm, or they have a valid exemption. From 25 October 2027, certain cryptoasset activities will become regulated activities requiring authorisation from the FCA. At that point, the exemption enabling MLR-registered cryptoasset business to communicate financial promotions will be removed. For more information see FCA, 2026. A new regime for cryptoasset regulation. [accessed 15 June 2026].

[91] See footnote 81 in paragraph 3.2.

- evidence of registration with the FCA for those promoting cryptoassets; or
- documentation demonstrating that a valid exemption applies.

3.37 The following box includes feedback provided by the FCA to Ofcom on common tactics deployed by bad actors where such checks are carried out, and the steps providers can take in response.

Example 3.3: FCA feedback on bad-actor tactics where approvals or exemptions apply, and how services may respond[92]

Common tactics flagged by the FCA include:

- claiming a promotion is FCA-approved or using phrases such as 'registered with the FCA';
- misusing the identity of an authorised firm (for example, quoting a FRN but linking to a clone website); and
- claiming exemptions (for example, 'for high-net-worth investors only') where exemption conditions are not met.

Possible provider responses to these tactics:

- verifying approval directly with the FCA-authorised firm by checking the authorised firm's FRN, name, contact details, and websites against the FCA Financial Services Register, asking it to pass verification themselves and to provide written confirmation that it has approved the advertisement;
- preventing cloning attempts by ensuring contact details and websites match official FCA Financial Services Register entries; and
- requiring evidence that any claimed exemption legitimately applies.

Repeating financial services verification

3.38 Providers should ensure that their view about whether an individual or firm is legally permitted to advertise financial services remains accurate over time. Once a provider has verified that an individual or firm is legally permitted to promote financial services, it need not repeat the verification process each time that individual or firm publishes a financial services advertisement, unless the permission applies only to a specific advertisement. Maintaining a record of verification outcomes would support this.

3.39 Where the provider has reason to suspect that an individual or firm may no longer be legally permitted to promote financial services, it should repeat the verification process. Such circumstances include, but are not limited to:

a) changes to authorisation status of the verified individual or firm promoting financial services;
b) material changes to an individual or firm's account information, such as contact details; or
c) the identification of suspicious activity associated with the firm or individual's account.

3.40 Providers should set out in their financial services verification policy the circumstances in which verification will be repeated, and the actions they will take as a result.

[92] FCA written response dated 3 March 2025 to Ofcom engagement on 17 February.

Action where verification is not passed (or financial services advertising is not permitted)

3.41 Where a provider identifies financial services advertising, whether through proactive detection or other means, the provider should check if the individual or firm which posted the advertisement has previously passed financial services verification. If the individual or firm has not, the provider should ensure that the advertisement is no longer available to UK users while verification is carried out.

3.42 If the individual or firm that posted the advertisement does not pass financial services verification, or the provider does not permit financial services advertising on its service, the provider should treat the advertising as suspected fraudulent advertising (or suspected fraudulent advertising proxy[93]). The provider should then review, assess and take appropriate action against it in line with Volume 4, Section 2, 'Advertising moderation'.

3.43 Financial services advertisements should only be allowed to be made available to UK users once the individual or firm promoting them has been successfully verified, and in line with the provider's policy.[94]

3.44 Where individuals or firms do not pass financial services verification, they can appeal this decision. Volume 3, Section 6, 'Account appeals' sets this out.

Review and update of the financial services verification policy

3.45 We expect service providers to review and update their financial services verification policy to ensure it is, and continues to be, effective at ensuring checks are completed on any individual or firm intending to advertise financial services on their service.

3.46 Providers should carry out the review and implement any subsequent updates at least every 12 months or if there is a significant change in the way advertising on the service operates.

3.47 Providers should keep a written record of annual reviews and of current and previous versions of its financial services verification policy so that they can track progress and learn from previous reviews.

3.48 We consider that all records should be kept for a minimum of three years (consistent with our Record-Keeping and Review Guidance), or in accordance with the organisation's record retention policies, if longer.[95]

Benefits and effectiveness

3.49 We consider that our proposal for financial services verification is an essential step in reducing online fraud, and safeguarding users against one of the highest-impact drivers of large-scale financial loss.[96] As set out in Volume 1, Section 4, 'Causes and impacts of

[93] A fraudulent advertising proxy is an advertisement that a service provider has assessed against its own categories of prohibited advertisements (set out in its terms of service or publicly available statement, advertising contracts (where all of the provider's advertising contracts contain similar prohibitions in relation to fraudulent advertisements), or a combination of these when read together). The provider may do this where it is satisfied that the fraudulent advertisements that it has reason to suspect exist are prohibited by these policies or contracts. For more information, see Volume 4, Section 2, 'Advertising moderation'.
[94] It is also possible that advertising moderation determines that some advertisements are not in fact financial services advertising at all and were a 'false positive' incorrectly identified.
[95] Ofcom, 2025 Record-Keeping and Review Guidance.
[96] See Volume 1, Section 4, 'Causes and impacts of fraudulent advertising', paragraph 4.23.

fraudulent advertising', financial frauds such as investment scams account for some of the largest losses across all fraud types and are increasingly popular amongst perpetrators. They are also likely to be carried out by individuals and firms advertising financial services without FCA authorisation or a valid approval or exemption. According to the Perimeter Report from the FCA, some of the most serious harm from investment scams continues to come from businesses operating without FCA authorisation.[97] This shows there is an overlap between investment fraud targeting UK users and illegal financial promotions.

3.50 We therefore consider that there is a clear benefit in proposing providers complete checks for FCA authorisation and the FCA Warning List to ascertain whether individuals and firms are legally permitted to post financial services advertising. There is strong evidence that this approach works. For example, according to the FCA, in 2021 Google achieved a near 100% initial reduction in financial scam advertisements after implementing a financial services verification policy to only allow advertisements from, or approved by, FCA-authorised firms to run in the UK.[98]

3.51 Recent evidence from other jurisdictions further points to financial services verification being effective and beneficial for reducing online financial fraud too. In 2024, the Taiwanese Government introduced regulations in the Fraud Crime Prevention Act requesting online advertising platforms to verify the identities and licenses of financial advertisers. Taiwan's Ministry of Digital Affairs observed that their efforts significantly reduced the rates of scam advertisements involving investments, citing in press statements a 96% drop.[99]

3.52 We also consider that an important benefit of our proposal is its expectation that providers take steps to find financial services advertising before this is able to be encountered by users, ensuring that individuals or firms promoting such content are subject to verification. This approach will help ensure that financial services advertisements are consistently identified and verified, including in cases where systems that may be in place (such as self-declaration alone) would not be effective in stopping bad actors attempting to evade checks by being dishonest about their intentions.

3.53 For example, in Australia, the Scams Prevention Framework Act 2025 requires providers to verify that all advertisers of financial products have an Australian financial services licence and to take steps to identify scam advertising and accounts.[100] We understand that, in instances, this expectation has enabled unverified financial advertisements to be successfully detected and stopped – outcomes that have not consistently been achieved in the UK under current voluntary approaches.[101]

---

[97] FCA Perimeter Report, 2024, referenced in FT Adviser, 2024. FCA: We do not always have the power to act. [accessed 15 May 2026].

[98] FCA, 2026. Reducing and preventing financial crime. [accessed 20 June 2026].

[99] The 96% reduction figure is based on information provided by Taiwan's Ministry of Digital Affairs to Reuters. The information provided does not specify the definitions used or the baseline for comparison, and the cited percentage may therefore reflect changes in detection, reporting or visibility of such advertisements. Source: Horwitz, J, 2025. Meta created 'playbook' to fend off pressure to crack down on scammers, documents show, Reuters, 31 December. [accessed 15 May 2026].

[100] Treasury of the Australian Government, 2025. Scams Prevention Framework. [accessed 25 May 2026].

[101] A test run by a Reuters reporter with a fabricated high-return investment advertisement on Facebook showed a clear difference in enforcement across jurisdictions. After Reuters deliberately did not declare the advertisement as financial services during the approval process, the advertisement was approved and allowed to run in the UK without additional scrutiny. In Australia, however, the same undeclared advertisement was

3.54 Finally, we consider that another benefit of our proposed measure is that it builds on existing efforts undertaken by many providers and therefore can be implemented effectively. We consider that the expectations in this proposed measure are consistent with commitments undertaken by providers under the Online Fraud Charter and current voluntary practice agreed with the FCA, which we would expect providers continue to honour.[102] [103]

Consultation on use of proactive technology to find financial services advertising

3.55 The proposed financial service verification measure will only work effectively when service providers are able to detect financial advertisements, and through this the accounts which are posting them that therefore need to go through verification. To achieve this, we provisionally consider that providers will need to deploy proactive technology which detects financial services advertisements prior to them being made available to UK users. We expect this would mean that all advertisements would need to be subject to detection processes before being shown to UK users. Human review alone is not suitable because providers in scope of the proposed measure host millions of advertisements a year.

3.56 We therefore intend to consult on a measure recommending that providers of Category 1 and 2A services use proactive technology to detect advertisements for financial services. We will consult on the detail of this proposed measure separately in autumn 2026. This is to enable us to ensure consistency in our policy on proactive technology in different areas.

3.57 In June 2025 we published our Additional Safety Measures Consultation on a number of potential expansions to our Codes of Practice, including proposals related to the use of proactive technology to detect illegal user-generated content, including user-generated fraud. We are currently analysing stakeholder feedback to that consultation and will publish a regulatory statement setting out the decisions we have taken on the matters covered in the June 2025 Consultation, including proactive technology, in autumn 2026. It makes sense to align the timing of our consultation on the use of proactive technology to detect advertisements for financial services with this statement.

Impacts and costs on service providers

Direct costs for service providers

3.58 We expect that service providers may incur one-off costs, as well as annual ongoing costs, where implementing our proposed measure on financial services verification.

3.59 In the following paragraphs, we consider the potential costs that providers may incur in relation to the main steps of our proposed measure if implementing these steps for the first

---

proactively blocked during review, and Reuters, as the advertiser, was required to prove authorisation from the Australian financial regulator before it could run the advertisement. Source: Seers, P., Reggiori Wilkes, T. and Horwitz, J. 2026. Exclusive: Meta vowed to stop illegal financial ads in Britain. It failed 1,000 times in a week, Reuters, 18 March. [accessed 25 May 2026].

[102] The Online Fraud Charter 2023 expects signatories to deploy measures to protect users from fraudulent advertisements. For firms with paid advertising services, this includes the expectation to confirm that UK regulated financial services companies are authorised by the FCA prior to serving their advertisements. Source: GOV.UK, 2023. Online Fraud Charter. [accessed 25 May 2026].

[103] The FCA highlights that Google, Bing (Microsoft), Meta, X and TikTok changed their policies to only permit paid-for advertisements for financial services, including investments, by an FCA-authorised person or firm. Source: FCA, 2026. Reducing and Preventing Financial Crime. [accessed 20 June 2026].

time. Where relevant, we consider the costs that could be incurred if providers were, at a minimum, to check individuals or firms advertising financial advertisements for FCA authorisation against the FCA Financial Services Register and Warning List.

Setting out a financial services verification policy

3.60 Service providers will need to specify the types of financial services advertising that are permitted and who is able to advertise them on their service, in their financial services verification policy. Providers will also need to publish a high-level summary of the policy.

3.61 We expect providers would need to dedicate staff time towards determining the specified aspects of the policy as well as drafting and obtaining sign-off on the policy from senior management and arrange for its publication. We assume this could require a small team consisting of two professional occupation staff members (for example, policy manager, legal employee) for three months and one content moderator for one month to determine the types of financial services advertising to permit and prohibit and information to publish; and half a day of a senior director's time to review and approve the policy. We estimate this could cost providers around £31,600 to £62,800.[104] However, these costs are likely to depend on providers' internal processes for developing, approving and publishing new policies, and therefore costs could be higher for some providers.

Finding financial services advertising, and the individuals and firms posting it

3.62 We consider that service providers should have the means to detect financial services advertising, as well as the individuals and firms posting it. As set out in paragraph 3.18, we intend to consult on a measure recommending that providers of Category 1 and 2A services use proactive technology to detect financial services advertisements in autumn 2026. We will set out our analysis of the costs of this proposed measure when we consult on it.

3.63 Providers would still retain the flexibility to use other methods to find financial services advertisers in addition to proactive technology if this aligns with their business needs. This could include continuing to use (alongside proactive technology) self-declaration from financial services advertisers as a method.

Verifying if the individual or firm is authorised by the FCA

3.64 To check if an individual or firm is authorised by the FCA we expect service providers will first need to access the Financial Services Register. They will then need to check whether details of the individuals and firms match against the Register. Finally, providers will need to verify that the individual or firm trying to advertise on their service is the individual or firm on the Register.

3.65 The FCA Financial Services Register is accessible manually, as well as via an API service and Register Extract Service (RES).[105] Access through manual searches and the API service are provided free of charge, whereas the RES is only accessible with a subscriber fee.[106] In the

[104] See our labour cost assumptions in in Annex 8 'Further detail on economic assumptions and analysis' for more information.

[105] The API service can provide information about a single entity at a time, whereas the RES is able to provide most of the information from the Financial Services Register as a series of files (in the form of bulk downloads). Sources: FCA, 2026. Financial Services Register Extract Service Subscribers' Handbook. [accessed 5 June 2026]; FCA, 2026. Financial Services Register. [accessed 5 June 2026].

[106] For firms regulated by the FCA, total fees can range from around £3,000 to £11,000 per year. For non-FCA-regulated firms, total fees can range from around £6,000 to £20,000 per year. The exact fees the service

following paragraphs, we consider the potential costs of providers accessing and checking for information such as the advertiser name (legal entity and trading name) and firm reference number using the API service. This is consistent with how some providers appear to access the FCA's Financial Services Register.

3.66 We expect that providers may at a high-level need to:

a) sign up to the FCA portal to obtain access to the APIs;
b) integrate the relevant APIs into their existing systems;
c) test and determine the level of accuracy at which matches of the advertiser details are returned; and
d) feed the matches back into onboarding processes.

3.67 We assume the initial work of accessing the APIs and setting up the infrastructure needed to return the matches may require full-time work from a software engineer for three months and full-time work from an IT project manager for one month to oversee the work. Based on this, we estimate a potential one-off set-up cost of around £22,800 to £45,600.[107] However, we expect that these costs could be higher for services with more complicated workflows.

3.68 Once set-up, we expect the potential ongoing costs of the API returning matches are likely to be low. However, this will depend on the type and level of accuracy of the matching, and on fraudsters' efforts to find ways to achieve close matches to authorised firms. If a long list of possible matches is returned, then further staff input may be needed to process the possible matches and find the strongest match.

3.69 There may be other ongoing costs in relation to maintaining the infrastructure, for example, to account for version updates in the API and new functionalities on services. We estimate a potential ongoing maintenance cost of around £5,700 to £11,400 per year.[108]

3.70 Once a match is found against the Financial Services Register, service providers should then verify that the individual or firm trying to advertise on their service is the individual or firm on the Register. A potential approach could be to ask the individual or firm promoting financial services to prove they can access an email address consistent with the individual or firm domain(s) found on the Financial Services Register, by confirming a one-time password sent to it.[109]

3.71 Providers could rely on third-party suppliers of one-time password authentication solutions to do this. As mentioned in in Volume 3, Section 2, 'Account checks and actions', subsection 'Impacts and costs on service providers', we expect there would be one-off set-up costs associated with integrating a third-party solution. Additionally, there would be ongoing costs based on the number of verifications undertaken per year. For a service provider

---

provider pays within these ranges will depend on the data scope and frequency of download. FCA, 2026. Obtaining a data extract from the Financial Services Register. [accessed 9 June 2026].

[107] See our labour cost assumptions in Annex 8 'Further detail on economic assumptions and analysis' for more information.

[108] Consistent with our standard assumptions as set out in Annex 8 'Further detail on economic assumptions and analysis', we assume that the ongoing maintenance costs are 25% of the initial one-off set-up costs.

[109] We are aware that email addresses can only be obtained through manual searches of the Financial Services Register rather than through automated means (API) to prevent potential misuse of this data. We therefore expect there would be some additional costs involved to providers if manually searching the Register.

onboarding around 1,000[110] financial services advertisers per year, we expect the cost of verifying the email address found on the Financial Services Register is likely to be very small (less than £100 per year).

Checking if the individual or firm appears on the FCA Warning List

3.72 We expect service providers will first need to access the FCA Warning List. They will then need to check whether details of the individuals and firms match against the FCA's Warning List.

3.73 The FCA Warning List is directly accessible via the FCA's website. It provides the functionality to manually search and filter for unauthorised firm names.[111] We expect there will be ongoing costs directly related to the time spent by staff to undertake the manual searches and checks to see if any of the account's information appears on the FCA Warning List. Service providers that onboard a large number of financial services advertiser accounts could opt to build a system that is able to regularly retrieve data from the FCA's Warning List, process the data into a searchable database, and test and integrate calls for the data to return possible matches. We expect this may be more complex and could require full-time work from one software engineer for three months and one IT project manager for one month, therefore producing one-off costs (around £22,800 to £45,600) and ongoing maintenance costs (around £5,700 to £11,400 per year) similar to that noted for checking the FCA Financial Services Register.

3.74 There could also be further ongoing costs associated with the ongoing ingestion of data from the FCA Warning List to ensure the database is kept up to date,[112] as well as the costs associated with potential data storage requirements.[113]

Verifying individuals and firms which are not authorised by the FCA and not on the Warning List

3.75 If providers allow financial services advertisements from individuals or firms not FCA-authorised and not on the Warning List, they should collect and verify additional evidence showing those parties are legally allowed to promote financial services. The cost of undertaking this verification is likely to vary by individual case, in particular the specific claims made by the individual or firm trying to advertise financial services and the evidence they are able to submit. Therefore, we have not sought to provide estimates of the potential costs that could be involved.

3.76 Compared to verifying advertisers on the Financial Services Register, the process of verifying this subset of advertisers is likely to be more complex and therefore could involve

---

[110] We have estimated this figure based on the average number of financial services advertiser accounts onboarded in 2024/25 by six providers. Sources: [✂] response to our formal information request issued 30 January 2026; [✂] response to our formal information request issued 30 January 2026; [✂] response to our formal information request issued 30 January 2026; [✂] response to our formal information request issued 30 January 2026; [✂] response to our formal information request issued 30 January 2026; [✂] response to our formal information request issued 30 January 2026.

[111] FCA, 2026. Warning List of unauthorised firms. [accessed 5 June 2026].

[112] We are aware that providers could subscribe to a really simple syndication (RSS) feed provided by the FCA for regular updates.

[113] However, we expect the potential data storage requirements are likely to be low based on the number of entries in the FCA's Warning List (around 18,000 firms as of April 2026). Source: FCA, 2026. Warning List of unauthorised firms. [accessed 30 June 2026].

more staff input and higher costs. However, we do not expect this subset of advertisers to represent many.[114]

Overall costs

3.77 Based on this analysis, we estimate total one-off costs of around £77,200 to £154,000, and total ongoing costs of around £11,400 to £22,800 per year. However, we have not estimated costs for all the potential work and variations that may be involved in implementing this measure (for example, the costs of verifying individuals and firms not FCA-authorised or on the Warning List).

3.78 Many large service providers (for example, [✂], [✂], [✂], [✂], [✂], [✂]) already appear to verify the FCA authorisation of individuals or firms which say they intend to post financial services advertisements.[115] These services are already likely to have incurred some of the relevant set-up and infrastructure costs associated with identifying individuals or firms advertising financial services, as well as accessing and checking their details against the FCA Financial Services Register and Warning List. Therefore, we expect the costs associated with our proposed measure to these service providers is likely to be lower than our estimates in paragraphs 3.67 to 3.77.

Impact on individuals and firms advertising financial services

3.79 We expect the impacts identified in Volume 3, Section 2, 'Account checks and actions', subsection 'Impacts and costs on service providers' are also likely to apply for individuals and firms advertising financial services. There could be a potential increase in time as well as resources for legitimate account holders to complete the relevant checks and achieve the necessary financial services verification. However, we consider that service providers will have the incentives to ensure the relevant checks are as quick and easy to complete as possible. We also consider that our proposed measure on account appeals (see Volume 3, Section 6, 'Account appeals') will act as a safeguard for legitimate actors that fail to achieve the necessary financial services verification at the first instance.

Rights assessment

Freedom of expression

3.80 As explained in Volume 1, Section 5, 'Approach to codes', subsection 'Approach to human rights assessments', Article 10 of the European Convention on Human Rights (ECHR) upholds the right to freedom of expression, which encompasses the right to hold opinions and to receive and impart information and ideas without unnecessary interference by a public authority. Article 10 is a qualified right, and we must exercise our duties under the Online Safety Act 2023 (the Act) in a way that does not restrict this right unless satisfied that is proportionate to the legitimate aim pursued. As noted within 'Approach to codes', we start

[114] As highlighted in an FCA report, many services currently restrict advertising to FCA-authorised advertisers only. We are aware that some providers also permit advertisements where they are approved by FCA-authorised firms or rely on applicable exemptions, in line with existing regulatory frameworks. Source: FCA, 2026. Reducing and Preventing Financial Crime. [accessed 20 June 2026].

[115] [✂] response to our formal information request issued 26 June 2025; [✂] response to our formal information request issued 26 June 2025; [✂] response to our formal information request issued 30 January 2026 ; [✂] response to our formal information request issued 26 June 2025; [✂] response to our formal information request issued 26 June 2025; [✂] response to our formal information request issued 26 June 2025.

from the position that the proposed measures are prescribed by law, in pursuit of a legitimate aim and correspond to a pressing social need.

3.81 We consider that the rights impacts on freedom of expression in relation to this proposed measure are similar to those we have outlined for the proposed measure in Volume 3, Section 2, 'Account checks and actions', subsection 'Rights Assessment'.

3.82 The proposed measure has the potential to impact on the freedom of expression rights of users, advertisers and providers of Category 1 and 2A services. We have focused on the potential impact on the freedom of expression rights of users and advertisers as we consider this is likely to be more significant.

3.83 We recognise that this proposed measure recommends providers carry out checks, in the form of providers referring to the FCA Financial Services Register and Warning List to ascertain if an advertiser is FCA-authorised or has a warning issued against them. We recognise that the proposed measure gives providers a degree of discretion as to what financial services advertisements they allow on the service, including who is permitted to post them. So, they may choose to: (a) only allow financial services advertising posted by those who are FCA-authorised; or (b) allow financial services advertising by others who are unauthorised provided that the provider can implement additional verification to confirm that the advertiser is not on the Warning List and can prove they are legally permitted to place financial advertising on the service (for instance, if the advertisement has been approved by an FCA-authorised firm, or is subject to a valid exemption).

3.84 Accordingly, providers may make commercial choices to set a stringent verification policy to comply with this proposed measure, which may impact individuals or firms who are legally permitted to post financial services advertising but cannot post them under the policy adopted by the provider. This may limit not only the right of individuals and firms to freely impart ideas (via posting financial services advertising) but also may impact users' right to receive information and ideas from such advertising, which may not otherwise have been prevented from being placed on the service. However, as noted in paragraph 3.83, this would be a result of the provider's choice to set its policy in that way (which is an exercise of its own right to freedom of expression), rather than something that our proposed measure specifically recommends. Further, as noted in paragraph 3.54, we understand that many service providers already choose to only allow financial services advertisements from individuals or firms that are FCA-authorised.

3.85 We also recognise the potential restriction on legitimate advertisers who are not on the Financial Services Register in circumstances where providers do not allow for financial services to be advertised on their services at all. In such instances we note that there is potential interference with the rights of freedom of expression of these legitimate advertisers. However, similar to the points discussed in in paragraphs 3.84, this would be a result of the provider's choice and is not something that our proposed measure directly recommends. Further, to fully mitigate this risk, the proposed measure would need to recommend that providers allow all financial services advertising except where it is expressly prohibited by relevant financial services fraud offences set out in the Act. However, given the complexity and context-specific nature of those offences, we do not consider this approach to be practicable. In addition, such an approach would not reflect current industry practice nor public commitments as noted in paragraph 3.54, and would be likely to undermine the effectiveness of the proposed measure by reducing providers' ability and incentives to apply preventative verification controls, thereby increasing the risk of harm to

users from fraudulent advertising. It may also unduly constrain providers' discretion to set their own advertising policies, including whether to restrict certain categories of advertising as part of their commercial (and editorial) freedom. Therefore, while we recognise that this approach could mitigate some risk of interfering with the freedom of expression of legitimate advertisers, we do not consider that it would be as effective as the measure we are consulting on.

3.86 We note that under this proposed measure, verification could be carried out by humans, via automated technology, or a combination of both. While any type of verification involves a risk of errors, verification which involves automated process may be particularly vulnerable to bias. As noted in paragraph 3.95 in relation to data protection, where the verification is based solely on automated processing (that is, there is no meaningful human involvement in the decision), and has a "legal or similarly significant effect" on a person, providers should consider their obligations under Articles 22A to D of the UK General Data Protection Regulation (GDPR)[116] and have regard to relevant Information Commissioner's Office (ICO) guidance.[117]

3.87 As noted in paragraph 3.18, in autumn 2026, we also intend to consult on a measure proposing that providers of Category 1 and 2A services use proactive technology to detect paid-for advertisements for financial services. We will consider the rights impacts of that measure as part of that consultation.

3.88 Providers must also comply with the data protection principles of accuracy, fairness and transparency; in our view these principles mitigate against the risk of disproportionate interferences with freedom of expression arising from processing of personal data during verification.

3.89 To the extent that interference arises, our proposed measure on appeals acts as an important safeguard for freedom of expression. As set out in Volume 3, Section 6, 'Account appeals' the proposed account appeals measure allows account holders to appeal against decisions taken by service providers following failed account checks and to provide additional information to providers, who may overturn any action taken in response to an appeal.

3.90 In addition, we note that individuals and firms who do not pass financial verification checks or who have additional restrictions will be more likely to be perpetrators of financial services fraud; where this is the case, they would receive minimal, if any, protection for freedom of expression that takes the form of a fraudulent advertisement.

3.91 In Volume 1, Section 4, 'Causes and impacts of fraudulent advertising', we set out the significant adverse impact of fraudulent advertising on users. The proposed financial services verification measure will help ensure that only individuals and firms who are legally permitted to advertise financial services can do so and is crucial in helping prevent fraudulent financial services advertising. To the extent that the proposed measures may interfere with the rights to freedom of expression of users, individuals and firms (as set out in paragraphs 3.81 to 3.86, and taking into account advertisers' ability to appeal, we

[116] Articles 22A to D were substituted for Article 22 by section 80(1) of the Data (Use and Access) Act 2025, with effect from 5 February 2026: see the Data (Use and Access) Act 2025 (Commencement No. 6 and Transitional and Saving Provisions) Regulations 2026, regulation 2(j), subject to regulation 5.
[117] See ICO, 2026 (in draft at the time of publication). Automated decision-making, including profiling. [accessed 10 June 2026].

consider the interference to be proportionate to the Act's legitimate objective of protecting individuals in the UK from fraudulent advertising (which the proposed measures are intended to help providers of Category 1 and 2A services to secure).

Data protection and privacy

3.92 As explained Volume 1, Section 5, 'Approach to codes', subsection 'Approach to human rights assessments', Article 8 of the ECHR confers the right to respect for an individual's private and family life. Article 8 is a qualified right, and we must exercise our duties under the Act in a way that does not restrict this right unless satisfied that is proportionate to the legitimate aim pursued. As noted in relation to freedom of expression, we start from the position that these proposed measures are prescribed by law, in pursuit of a legitimate aim and correspond to a pressing social need. Article 8 underpins the data protection laws with which service providers must comply.

3.93 We recognise the requirement for providers to check the FCA Financial Services Register and the FCA Warning List is likely to give rise to a privacy impact. However, such impacts are likely to be very limited as providers will be mostly accessing publicly available information.

3.94 We consider that the privacy impacts from this proposed measure are broadly the same as set out in Volume 3, Section 2, 'Account checks and actions', subsection 'Data protection and privacy', in the context of the proposed measure recommending that providers set out how they will verify individuals and firms seeking to promote financial services to UK users. In implementing this measure in practice, providers will need to carry out checks on such individuals and firms, including any repeated checks as required.

3.95 Further, we consider that, depending on the systems and processes used by providers, the financial services verification checks that providers will need to carry out as part of this proposed measure are likely to involve the processing of personal, and potentially special category data of individuals and those working for or on behalf of firms, intending to post financial services advertising on services. The UK GDPR places specific restrictions on making decisions based solely on automated processing of personal data, where the decision has legal or similarly significant effects. These restrictions are imposed by Articles 22A to D of the UK GDPR.[118] So-called automated decision-making is permitted where service providers have appropriate safeguards in place. Additional restrictions also apply in relation to cases where special category data is used. The ICO has provided guidance on these matters.[119]

3.103 As noted in paragraph 3.18, we also intend to consult in autumn 2026 on a measure recommending that providers of Category 1 and 2A services use proactive technology to identify advertisements for financial services. We will consider the rights impacts of that measure as part of that consultation.

3.104 Service providers should ensure they, or any third parties that they outsource to, act in accordance with data protection legislation and relevant ICO guidance and consider the data protection principles of fairness, transparency and data minimisation in implementing this

[118] Articles 22A to D were substituted for Article 22 by section 80(1) of the Data (Use and Access) Act 2025, with effect from 5 February 2026: see the Data (Use and Access) Act 2025 (Commencement No. 6 and Transitional and Saving Provisions) Regulations 2026, regulation 2(j), subject to regulation 5.
[119] See ICO, 2026 (in draft at the time of publication). Automated decision-making, including profiling [accessed 10 June 2026].

proposed measure.[120] Providers will also need to ensure that data protection impacts are limited to what is necessary for the legitimate purpose of complying with the fraudulent advertising duties. We consider that safeguards under data protection law, as explained in the various pieces of ICO guidance, will help ensure that the impact of processing (including automated processing) on data protection and privacy rights is minimised.

3.105 To the extent that the proposed measure involves interference with account holders' rights to privacy, we consider the interference to be proportionate to the Act's legitimate objective of protecting individuals in the UK from fraudulent advertising (which these proposed measures are intended to help providers of Category 1 and 2A services to secure).

Provisional conclusion

3.106 All Category 1 and 2A service providers must have in place proportionate systems and processes designed to protect users from fraudulent advertising in accordance with their duties under sections 38(1) and 39(1) of the Act. Our proposed approach is to recommend providers carry out financial services verification as an important preventative step to protect UK users from fraudulent financial advertising.

3.107 For the reasons we have set out, we provisionally consider that the proposed checks would be effective at combatting fraudulent advertising and would deliver material benefits.

3.108 We expect that the proposed measure could result in some costs and may have impacts on the rights of advertisers. However, our provisional assessment is that these impacts would be proportionate, given the scale of harm caused by fraudulent financial advertising and the important role this proposed measure could play in addressing it.

3.109 Our provisional view is therefore that it is proportionate to recommend that Category 1 and Category 2A service providers carry out financial services verification.

3.110 The full text of the proposed measure can be found in the draft Fraudulent Advertising Code of Practice for user-to-user services and in the draft Fraudulent Advertising Code of Practice for search services, and it is referred to as FAU H2 and FAS H2 respectively.

[120] See ICO, no date. UK GDPR guidance and resources. [accessed 22 May 2026]. In the context of these proposed measures, in some instances this may involve 'storage and access technologies' which engage the requirements set out in regulation 6 of the Privacy and Electronic Communications Regulations (PECR). The ICO has also provided guidance on this matter. See ICO, 2026. Guidance on the use of storage and access technologies. [accessed 22 May 2026].

4. Countering account takeover

What is this section about?

Countering account takeover involves preventing bad actors from gaining access to legitimate advertisers' existing advertising accounts and using the accounts to post fraudulent advertisements. It also involves providing a way for legitimate account holders to report when one of their accounts has been taken over by a bad actor.

In this section, we set out our proposed measures for countering account takeover, and why we are proposing to recommend them.

Our proposals

Number in our Codes	Proposed measure applicable to providers of Category 1 and 2A services
FAU H3 and FAS H3	Providers should **implement an account security mechanism** on all advertising accounts.
FAU H4 and FAS H4	Providers should make available an **account takeover reporting mechanism that is easy to find, easy to access and easy to use.** This includes considering the accessibility of the reporting mechanism.

Why are we proposing this?

One technique fraudsters use is taking over legitimate advertising accounts and using them to post fraudulent advertisements. Fraudsters will be less able to do this where service providers have an effective security mechanism. Similarly, where account takeover does occur, having a reporting mechanism helps ensure providers are informed and can act swiftly to prevent further dissemination of fraudulent advertisements. As a result, we consider that having these systems and processes in place will be effective at assisting providers to comply with their duties under the Act to protect individuals in the UK from fraudulent advertising.

Consultation questions

- Do you agree with our proposals? Please confirm which proposed measure your views relate to and provide any arguments and supporting evidence.
- Do you have any evidence about account takeover that could inform our assessment, including how frequently it occurs or its impact?

Introduction

4.1 We propose that Category 1 and 2A service providers (providers) should implement two measures to prevent and tackle account takeover:

a) an account security mechanism on all new and existing advertising accounts; and

b) a reporting mechanism that enables advertising account holders to report suspected account takeover.[121]

4.2 Account takeover occurs when a bad actor gains access to an existing account owned by another account holder and takes control of it. Account takeover is one form of account compromise, a broader concept that also includes scenarios such as an authorised user misusing their legitimate access. Our proposed measures apply specifically to preventing and responding to account takeover.

4.3 We consider that account takeover could result in a bad actor being able to post fraudulent advertisements or a fraudulent advertising proxy via an advertising account.[122]

4.4 In this section, we outline and examine our two proposed measures. We explain how these proposed measures would work, set out our assessment of the proposed measures' benefits and effectiveness, and assess the impacts we consider they would have.

4.5 We acknowledge that a Category 1 or 2A service may be serving paid-for advertisements to its users through different advertising pathways. Where relevant, the proposed advertising intermediaries measure would apply. The proposed advertising intermediaries measure recommends that a provider should use all reasonable endeavours to implement a version of any measures it has been unable to apply. For more information, see Volume 2 Section 2, Advertising Intermediaries.

Account security

Explanation of the proposed measure

4.6 We are proposing to recommend that service providers implement an account security mechanism. The main aspects of this proposed measure are set out in paragraphs 4.8 to 4.23. Specifically, the mechanism should:

a) be implemented on all new and existing advertising accounts;
b) be implemented having regard to a set of factors which we describe in paragraphs 4.9 to 4.18;
c) be reviewed at least every 12 months, including carrying out appropriate security testing, or in response to material changes or emerging risks relating to advertising on the service; and
d) include a means for account holders to restore access to their accounts where access is lost.

4.7 We address these considerations in more detail in the following sub-sections.

[121] See Annex 7, 'Glossary' for our definition of 'advertising account holder' and Volume 1, Section 3, 'Online advertising ecosystem' for more information about the different types of persons who may use an advertising account.

[122] A fraudulent advertising proxy is an advertisement that a service provider has assessed against its own categories of prohibited advertisements (set out in its terms of service or publicly available statement, advertising contracts (where all of the provider's advertising contracts contain similar prohibitions in relation to fraudulent advertisements), or a combination of these when read together). The provider may do this where it is satisfied that the fraudulent advertisements that it has reason to suspect exist are prohibited by these policies or contracts. For more information, see Volume 4, Section 2, 'Advertising moderation'.

Implement on all new and existing advertising accounts

4.8 This proposed measure recommends that service providers should implement an account security mechanism on all advertising accounts on their service(s). This includes new and existing advertising accounts.

Implement a mechanism having regard to a set of factors

4.9 We have taken a principles-based approach by setting out factors for service providers to consider, rather than prescribing particular security mechanisms. While we do not specify a single mechanism, this includes measures such as multi-factor authentication (MFA), passkeys, and similar forms of strong authentication.[123]

4.10 When implementing an account security mechanism, service providers should consider the factors outlined in the rest of this sub-section. Some pertain to how the mechanism is developed and must be considered when making a selection.

Mechanism protects against unauthorised access

4.11 The service provider should ensure that the mechanism is designed to minimise the possibility that users other than permitted account holders can access the advertising account.

4.12 In practice, this means adopting mechanisms that are resilient against common methods of unauthorised access. This may need a layered approach. We provide an illustrative example from the banking sector to demonstrate how layered security mechanisms are implemented in practice.

Example 4.1: Layered checks in the banking sector

The banking sector typically applies layered account security mechanisms rather than relying on a single control. A baseline set of protections is commonly in place, with additional layers introduced where higher risk is identified. For example, in higher-risk situations, banks may apply an extra security layer, sometimes referred to as 'step-up' authentication, before allowing certain actions to proceed. This illustrates how, in other industries, multiple layers of security may be combined and applied flexibly depending on risk.[124]

Mechanism aligns with industry standards and good practice

4.13 The service provider should have regard to the effectiveness of the mechanism adopted, considering, at a minimum, consistency with existing industry standards and good practice.

4.14 We consider that it is important that the account security mechanism a service provider implements is robust against the tactics used by bad actors to gain access to advertising accounts and that it is designed to only allow access to permitted account holders. To support this, providers should consider up-to-date material from relevant UK government departments, agencies, law enforcement bodies and industry good practice.[125] This material

[123] Multi-factor authentication (MFA) verifies identity by requiring at least two distinct proofs. Instead of relying solely on a password, MFA adds additional layers of protection.
[124] IBM, 2025. Building smarter fraud defenses for banks | IBM. [accessed 26 June 2026]; Entrust, no date. What Step-up Authentication Is and Why It's Important for Identity. [accessed 18 May 2026].
[125] Cabinet Office and Government Digital Service, 2020. Using authenticators to protect an online service (Good Practice Guide 44). [accessed 8 April 2026]; National Cyber Security Centre (NCSC), 2024. Multi-factor authentication for your corporate online services. [accessed 8 April 2026]; National Institute of Standards and

should inform their understanding of what constitutes a robust account security mechanism and the circumstances in which different mechanisms are appropriate.

Mechanism is responsive to emerging risks and resilient to circumvention

4.15 The service provider should also consider the extent to which the mechanism reflects emerging risks and trends in the account security industry.

4.16 The account security landscape is constantly evolving, with good practice developing in tandem. Bad actors often identify ways to circumvent existing security standards, while new mechanisms are introduced, reducing the effectiveness of earlier approaches. Service providers should therefore ensure that their chosen mechanisms remain responsive to emerging risks and trends.

4.17 Service providers should also consider their account security mechanism within a broader context of known fraud techniques and relevant industry learning. This includes identifying potential points of circumvention and implementing appropriate controls to prevent, detect and respond to such activity.

4.18 We consider that service providers should have the flexibility to determine the type of account security mechanism that is most appropriate for their circumstances. However, the security mechanism implemented should reflect the factors set out in paragraphs 4.9 to 4.18 and support the purpose of this proposed measure, which is to reduce the risk of accounts being taken over.

Review at least every 12 months

4.19 We propose to recommend that service providers review their mechanism at least every 12 months, including carrying out appropriate security testing.

4.20 Providers should also review or update the mechanism in response to technological developments, shifts in patterns of fraudulent or unauthorised activity, or emerging risks.

Provide a mechanism for restoring access

4.21 We propose to recommend that service providers should have a way for advertising account holders who can no longer access their account to restore access.

4.22 International security standards and guidance recommend that organisations put appropriate account recovery procedures in place, and we understand that most service providers already operate some form of account recovery.[126]

4.23 We recognise that account recovery processes can be targeted by bad actors seeking to gain unauthorised access to advertising accounts. Service providers should therefore ensure that account recovery processes are robust and designed to prevent malicious access.

Technology (NIST), 2025. NIST SP 800-63-4: Digital Identity Guidelines. [accessed 8 April 2026]; Information Commissioner's Office (ICO). Passwords in online services. [accessed 8 April 2026].

[126] International Organization for Standardization, 2022. ISO/IEC 27001:2022 - Information security management. This standard sets out how organisations should implement and continuously improve information security management system; NIST, 2025. NIST SP 800-63-4: Digital Identity Guidelines. [accessed 8 April 2026]; OWASP Foundation, 2025. Application Security Verification Standard (ASVS) v5.0. [accessed 8 April 2026]; Google, no date. Use a passkey to log into your Google Ads account.[accessed 18 May 2026]; Facebook, no date. What can I do if I've lost access to my account? [accessed 18 May 2026].

Benefits and effectiveness

4.24 Account takeover is a known tactic used by bad actors.[127] Industry and civil society evidence indicates that it is particularly attractive because it allows bad actors to bypass onboarding and verification checks, making it easier to post fraudulent advertisements.[128] Ofcom research suggests that account takeover is also appealing because users are more likely to trust established brands.[129] Evidence indicates that reports of account takeover in general are increasing, and the consequences for users and services can be severe.[130]

4.25 We recognise that many service providers already offer account security measures, such as MFA.[131] Ofcom research shows that account security and takeover responses rely heavily on user initiative, with weak protections.[132] In practice, optional security features are not always enabled, even when they provide stronger protection. We are therefore proposing to recommend that account security measures are applied to all advertising accounts, so that a consistent level of protection applies across the board and accounts are less vulnerable to fraud.

4.26 Government guidelines recommend adding extra layers of account security to improve protection, as passwords alone are often insufficient to provide a high level of security.[133] Evidence also demonstrates that security measures such as MFA are widely regarded as a means to reduce the chance of account takeover when implemented in a way that does not create excessive barriers for legitimate account holders.[134]

---

[127] LinkedIn response to our formal information request on costs issued 30 January 2026; Microsoft response to our formal information request on costs issued 30 January 2026; [✂] response to our formal information request on costs issued 30 January 2026; Romero, J., 2021. Combating e-commerce scams and account takeover attacks, Meta Newsroom, 29 June. [accessed 6 May 2026]; Cifas, 2025. Fraudscape 2025: Reported fraud hits record levels. [accessed 6 May 2026].

[128] Which? response to 2024 Call for Evidence: Third Phase of Online Safety Regulation (2024 Call for Evidence); UK Finance response to 2024 Call for Evidence, p.20. See Volume 1, Section 4, 'Causes and impacts of fraudulent advertising';[✂] response to 2024 Call for Evidence; We are aware that the proportion of fraudulent advertisements detected and originating from compromised accounts varies widely across individual services in a given year, from around [✂] for [✂] to [✂] for [✂] and [✂] for [✂]. [✂] response to our formal information request issued 30 January 2026; [✂]response to our formal information request issued 30 January 2026; [✂] response to our formal information request issued 30 January 2026]; [✂]response to our formal information request issued 30 January 2026; [✂] response to our formal information request issued 30 January 2026; [✂] response to our formal information request issued 30 January 2026.

[129] Ofcom, 2026. Online paid-for advertisements research.

[130] Cifas, 2025. Fraudscape 2025. [accessed 9 February 2026]; Major warning issued after surge in social media and email account hacks – how to protect yourself, Independent, 17 March. [accessed 19 June 2026]; Cifas, 2026. This is Fraudscape 2026. [accessed 16 March 2026]; Revolut (confidential) response to 2024 Call for Evidence.

[131] TikTok, 2025. Best practices for securing your account. [accessed 18 May 2026]; LinkedIn, 2025. Two-factor authentication Campaign Manager FAQs. [accessed 18 May 2026]; Meta, no date. Verification requirements for advertisers. [accessed 18 May 2026]; X, no date. How to use two-factor authentication. [accessed 18 May 2026]; Pinterest, no date. Two-factor authentication for business. [accessed 18 May 2026]; Google, no date. Secure your Google Ads account: Introduction. [accessed 18 May 2026].

[132] Ofcom, 2026. Behavioural audit of services with advertisement functionality.

[133] Cabinet Office and Government Digital Service, 2020. Using authenticators to protect an online service (Good Practice Guide 44). [accessed 6 May 2026]; NCSC, 2024. Multi-factor authentication for your corporate online services: Recommended types of MFA. [accessed 6 May 2026].

[134] AGENCY response to 2024 Call for Evidence, p.15; Advertisers explained that multi-factor authentication was widely accepted as a standard expectation when managing any digital account, not just in online advertising and they regularly use it. Ofcom, 2026. Online advertising pathways: qualitative research report.

4.27 Recognising the rapidly evolving nature of security mechanisms in this area, the National Cyber Security Centre has also indicated a preference for passkeys where services support them, and for two-factor verification where they do not. This position reflects growing evidence that stronger authentication methods provide better protection against account compromise than passwords alone.[135]

4.28 While industry already uses a range of account security mechanisms, bad actors continually adapt their techniques to bypass existing controls. As a result, security measures can become less effective over time if they are not regularly reviewed and updated. Using up-to-date methods and updating them to reflect emerging techniques increases the likelihood that these controls remain effective.

4.29 We consider that if service providers review their chosen account security mechanism at least every 12 months, this would help ensure it continues to reflect industry standards and good practice.

4.30 By making account takeover materially more difficult, the proposed measure is expected to reduce the volume of fraudulent advertising on Category 1 and Category 2A services, compared with a scenario in which these protections are not adopted.[136]

4.31 Account takeover is typically responsible for between [✂] of fraudulent advertising. We therefore estimate that account takeover causes up to tens of millions of pounds worth of harm to UK consumers and businesses each year.[137] Since some service providers have already taken steps which partially meet the recommendations of the measure, the harm account takeover does to consumers would be worse still in a counterfactual where service providers were not taking any steps to follow the measure. This suggests that there is scope for this proposed measure to deliver substantial benefits for UK consumers. The magnitude of such benefits however will largely depend on how service providers implement our proposed measure, and therefore the extent to which account takeovers will be constrained in practice.

4.32 This proposed measure works closely with other proposed measures in the draft Fraudulent Advertising Codes, especially those on advertising account checks and advertising bans.[138] The introduction of the account checks measures proposed in Volume 3, Section 2, 'Account checks and actions', may increase attempts by bad actors to take over accounts in order to bypass strengthened controls. We have designed the proposed account security measure to address this concern by adding a further layer of protection for advertising account holders and a corresponding barrier for bad actors.

4.33 Helping account holders recover compromised accounts should also help to prevent users from encountering fraudulent advertisements, as bad actors can be stopped more quickly from using compromised accounts to post advertisements. A strong account security mechanism that helps advertising account holders protect and recover compromised

---

[135] Chismon, D., 2026. Passkeys are more secure than traditional ways to log in, National Cyber Security Centre blog, 23 April. [accessed 6 May 2026]. NCSC, 2026. Leave passwords in the past - passkeys are the future. [accessed 26 June 2026].

[136] Ten-year Net Present Value (NPV) using HM Treasury's 3.5% discount rate as detailed in The Green Book. HM Treasury, 2026. The Green Book: UK Government Guidance on Appraisal, p.46. [accessed 18 June 2026].

[137] We have obtained these estimates by multiplying the percentages (proportion of fraudulent advertising coming from account takeovers, that is, [✂] with our estimates of the overall harm which we detail in Annex 8, 'Further detail on economic assumptions and analysis'.

[138] Volume 3, Section 2, 'Account checks and actions', and Volume 3, Section 5, 'Advertising bans'.

accounts should also reduce the potential costs of account takeover for legitimate account holders. We discuss account recovery in paragraphs 4.21 to 4.23, and 4.88 to 4.92.

4.34 We have adopted a principles-based approach rather than recommending specific security mechanisms. This reflects the fact that fraud tactics used by bad actors evolve rapidly, and account security measures must be capable of adapting in response. A prescriptive approach risks becoming outdated or ineffective, whereas the framework of factors set out in paragraphs 4.9 to 4.23 gives providers the flexibility to implement and update controls that are appropriate to the risks they face, while maintaining robust protection against unauthorised access.

Impacts and costs on service providers

Direct costs for service providers

Choosing an account security mechanism

4.35 Service providers may incur some initial costs to assess which account security mechanism to implement. These costs would mainly be in the form of staff time, for example, to research and examine existing good practices, emerging risks and trends in the account security industry, as well as consider the appropriateness of different mechanisms and what information could be published about the mechanism chosen. We estimate this could involve an initial one-off cost to services of around £28,000 to £55,500.[139]

4.36 There will likely also be ongoing costs associated with service providers reviewing or updating the mechanism in response to technological developments or new emerging risks and trends. In line with standard assumptions, we assume these costs to be 25% of the initial one-off costs and we therefore estimate a cost of around £7,000 to £13,900 per year.[140] However, these costs could be higher if more substantial updates are required to the mechanism chosen.

Implementing an account security mechanism

4.37 In practice many Category 1 and 2A service providers already have account security mechanisms in place and also publish information about how the mechanisms work. Google, Meta, TikTok and X appear to provide two-factor authentication (a form of MFA) for advertising accounts.[141]

4.38 For the purpose of this analysis, we focus on the potential costs associated with service providers implementing MFA. We use MFA as our illustrative example of an account security mechanism, to reflect current industry practice. For a service provider implementing MFA, there are a range of methods available to them in the market, at different price points.

---

[139] We assume it takes two full-time professional occupation staff members around three months to undertake the relevant research, and half-time from one senior director for one day to review the research and approve the mechanism chosen. See Annex 8, 'Further detail on economic assumptions and analysis', Further detail on economic assumptions and analysis.

[140] See Annex 8, 'Further detail on economic assumptions and analysis'

[141] TikTok, 2025. Best practices for securing your TikTok for Business account. [accessed 6 May 2026]; Google, no date. Secure your Google Ads account: Introduction. [accessed 6 May 2026]; Meta, no date. Verification requirements for advertisers. [accessed 6 May 2026]; X, no date. How to use two-factor authentication. [accessed 6 May 2026].

4.39 An example of a low-cost method is using MFA via authenticator apps. We are aware that many service providers currently use this method.[142] This method involves minimal ongoing costs for providers because there is no cost per account or per MFA application. This means it is a low-cost option for providers with a large number of advertising accounts. However, providers may incur other related ongoing costs. For example, where advertising account holders are incorrectly locked out of accounts due to authentication errors, providers may receive and have to deal with such support requests.

4.40 There are also more expensive methods available in the market. For example, service providers could adopt MFA as part of wider, security and access management solutions that are provided by third-party suppliers.

4.41 In this case, there would be one-off costs associated with onboarding and integrating the third-party supplier into existing systems; integrating any relevant APIs provided by the third party; and undertaking testing, as well as security and compliance reviews. We estimate these steps could take at least three months of full-time work by a software engineer and the equivalent time for a professional occupation staff member (for example, a policy manager), reaching one-off costs in the tens of thousands of pounds for services. There may also be annual maintenance costs associated with maintaining the integration with the third-party supplier over time. We estimate these costs could reach around the thousands or low tens of thousands of pounds per year.

4.42 There would also be other ongoing costs, in relation to the prices charged by the third-party supplier. These third-party suppliers typically operate on a pay-per-user pricing model, with costs increasing with the number of advertising accounts on services. Therefore, costs could be substantial for large services, potentially reaching a few millions of pounds per month.[143] However, these costs do not only reflect the cost of implementing MFA, but also the range of other services provided in these solutions, which go beyond the requirements of our proposed measure.[144] It is also likely that some suppliers may offer volume-based discounts, which could help lower the cost per advertising account.[145]

4.43 This analysis only provides an indication of some of the options available in the market. Overall, service providers will have flexibility to choose from the available options in the

---

[142] We are aware of providers that already offer such authentication apps as an option of a second form of verification to those who manage or use accounts. For example, LinkedIn provides account holders the option of phone number (SMS) or an authenticator app. Source: LinkedIn, no date. Two-factor authentication Campaign Manager FAQs. [accessed 12 June 2026]. TikTok provides account holders the option of text message (SMS), email or third-party authentication app. Source: TikTok, 2026. About 2-step verification in TikTok Ads Manager. [accessed 12 June 2026]. X provides account holders the option of text message, authentication app or security key. Source: X, no date. How to use two-factor authentication. [accessed 12 June 2026].

[143] Based on the publicly available price points of three third-party suppliers, we consider the likely price per advertising account per month for such solutions could range from around £2 to £5. Sources: Cisco Duo, no date. Compare Duo editions and pricing. [accessed 30 March 2026]; Microsoft, no date. Microsoft Entra ID. [accessed 30 March 2026].

[144] This includes services such as single sign-on, password-less authentication, event logging and reporting, and so on.

[145] Based on some publicly available information, we are aware of suppliers having offered volume discounts for MFA solutions, with a 20% discount for user volumes of around 1,000 to 5,000 and a 30% discount for user volumes of more than 5,000 users. We provide this only as an indicative example of the type of discounts that could be applied, but we are aware that such discounts (where available) are more likely to be the outcome of bilateral negotiations. Source: Quadris, no date. G-Cloud 14 Framework. Lot 2: Cisco Based Services Pricing. [accessed 2 June 2026].

market, and it would be a commercial matter for them whether they chose a low or a high cost solution. For the purposes of assessing whether this proposal is proportionate, we have placed more weight on the existence of lower cost options for implementing the proposed measure.

Overall costs

4.44 As MFA is currently the industry standard, we consider that most service providers will likely already have it in place and therefore have incurred the relevant one-off costs of doing so. Depending on how the provider currently uses MFA, they may incur additional costs to ensure it aligns with our proposed measure. For example, if MFA is not provided and applied to all accounts, these providers may need to incur additional development and testing costs so that the MFA is set up to work across all advertising accounts.[146] We do not expect these costs to be substantial, but the additional work needed would depend on how the provider has implemented MFA in the first place. Similarly, we expect the additional ongoing costs providers may incur would be in line with the additional number of advertising accounts that would need to adopt MFA.

Impact on account holders

4.45 As most Category 1 and 2A service providers currently provide account security mechanisms on an optional basis, we have considered the potential risk that our proposed measure could create additional friction for some advertising account holders who currently do not use such security mechanisms on their accounts.

4.46 However, we think this additional friction is likely to be justified in the context of the additional protection the account security mechanism can provide to advertising accounts, for example, by lowering the risk of potential account compromises and unauthorised access and also the potential costs associated with legitimate account holders having to deal with account takeovers. We further consider the additional friction to be justified, as by making account takeovers materially more difficult, the proposed measure is expected to reduce the volume of fraudulent advertisements and therefore protect users.

4.47 A strengthened security mechanism can also help safeguard the integrity of advertising campaigns, prevent misuse of advertising budgets, help advertising account holders maintain trust in services, and therefore create a more secure environment for account holders overall.

Rights assessment

Freedom of expression and freedom of association

4.48 As set out in Volume 1, Section 5, 'Approach to codes', Article 10 of the European Convention on Human Rights (ECHR) upholds the right to freedom of expression, which encompasses the right to hold opinions and to receive and impart information and ideas without unnecessary interference by a public authority. Article 10 is a qualified right, and we must exercise our duties under the Online Safety Act 2023 (the Act) in a way that does not restrict this right unless satisfied that is proportionate to the legitimate aim pursued. As noted in 'Approach to Codes', we start from the position that this proposed measure is prescribed by law, in pursuit of a legitimate aim and corresponds to a pressing social need.

[146] This may involve changes to their existing user interfaces, as well as onboarding and login workflows, to ensure they fully integrate MFA.

4.49 This proposed measure may engage the Article 10 rights of users as recipients of advertising content; service providers in determining how advertising appears on the service and is moderated; and advertisers, to the extent they use the service to communicate commercial messages. In this assessment we have focused on the rights of advertisers, because we consider the impact on their Article 10 rights is likely to be more significant as a result of the proposed account security mechanism.

4.50 We recognise that the proposed measure will interfere with account holders' rights where service providers act against an account because of actions or checks designed to prevent account takeover. This proposed measure should aid in blocking bad actors from implementing account takeover, but we recognise that checks may also block an account holder from accessing their account, for example, where account security details are entered incorrectly. However, this should only be a temporary impact, and should be limited in practice as account holders s will be able to regain access to their account through the proposed recommendation that providers include an account recovery mechanism, which acts as a safeguard to the right to freedom of expression. In addition, we think that this impact is proportionate to the benefits arising from the proposed measure, and will be mitigated by the recommendation to regularly review and test the effectiveness of the account security mechanism.

4.51 Service providers should think about the needs of their advertising account holders when deciding how to put this proposed measure in place. This includes both current account holders and people who may use the service in the future. The proposed measure should be implemented in a way that interferes as little as possible with people's rights. Providers will have commercial incentives to retain advertisers on their platform, and they will likely pay particular attention to advertisers who may join the service in future, especially where the proposed measure could discourage or prevent them from joining.

4.52 We consider that the proposed measure may also positively affect the right to freedom of expression. Increased account security should reduce the likelihood that an account is subject to account takeover by a fraudulent advertiser, thereby preventing the dissemination of fraudulent advertisements and the consequential damage arising from such advertising. The proposed measure may also contribute to increased confidence in advertising for consumers, where advertising accounts are less likely to be subject to account takeover.

4.53 As set out in paragraphs 4.24 to 4.34, we consider that this proposed measure should effectively reduce the volume of fraudulent advertisements disseminated on Category 1 and Category 2A services by preventing bad actors from taking over trusted accounts. The proposed measure also includes several factors service providers should consider when setting their account security policy, including regularly reviewing their policy and ensuring it reflects industry good practice.

4.54 We acknowledge that this proposed measure will involve an interference with advertisers' rights where they are prevented from accessing a service. However, we consider that the interference will be limited, and proportionate to the Act's legitimate objective of protecting individuals in the UK from fraudulent advertising.

Data protection and privacy

4.55 As explained in Volume 1, Section 5, 'Approach to Codes', Article 8 of the ECHR confers the right to respect for an individual's private and family life. Article 8 is a qualified right, and we must exercise our duties under the Act in a way that does not restrict this right unless

satisfied that is proportionate to the legitimate aim pursued. As noted in relation to freedom of expression, we start from the position that this proposed measure is prescribed by law, in pursuit of a legitimate aim and corresponds to a pressing social need. Article 8 underpins the data protection laws with which service providers must comply.

4.56 We recognise the proposed measure will interfere with right to privacy where service providers collect and process personal data for the purpose of account security checks. Our proposed measure does not specify the technological implementation of the proposed measure, and the extent of any interference with individuals' right to privacy will depend on the mechanism chosen by providers to align with the proposed measure, and may involve personal or biometric data.[147]

4.57 In implementing this proposed measure, service providers must also comply with data protection laws, ensuring they process no more data than necessary and do not retain it longer than is necessary to operate their account security mechanisms. Providers should also comply with all aspects of the UK General Data Protection Regulation (GDPR), and consider appropriate ICO guidance when implementing this proposed measure. Appropriate guidance may include the ICO's guidance on processing special category data, the ICO's guidance on online safety and data protection, and the ICO's guidance on automated decision-making.[148]

4.58 Service providers are required to comply with data protection legislation when implementing this proposed measure. This will include publishing information about their account security mechanism as part of their privacy notice, as required by the UK GDPR.[149]

4.59 We recognise that publishing too much detail could assist bad actors by revealing how security mechanisms operate. We therefore expect service providers to publish information at a sufficiently high level, without disclosing details that could be misused.

4.60 Overall, we acknowledge that this proposed measure will involve interference with individuals' right to privacy where their information is processed as part of account security checks. We consider the interference to be limited and proportionate to the Act's legitimate objective of protecting individuals in the UK from fraudulent advertising.

Provisional conclusion

4.61 Our provisional view is that it is proportionate to recommend that service providers implement an account security mechanism on all advertising accounts. Doing so would help reduce the risk of accounts being taken over by bad actors.

4.62 Putting appropriate security mechanisms in place should make account takeovers much more difficult. This should reduce the number of successful takeovers and help limit fraudulent advertising by removing a common method used by bad actors, compared with a situation where no such protections are in place.

---

[147] Biometric data is a type of personal data which is categorised as special category data. Processing of this data will require more protection, and providers processing biometric data should have regard to the ICO's guidance on processing special category data. Source: ICO, 2024. Special category data. [accessed 6 May 2026].
[148] ICO, 2026. Automated decision-making, including profiling. [accessed 9 June 2026] [ICO guidance is in draft at time of publication]; ICO, no date. Online safety and data protection. [accessed 6 May 2026].
[149] Articles 12 to 14 of the UK GDPR.

4.63 We also recognise that stronger checks on advertising accounts will make it harder for bad actors to operate and could lead to more attempts to break into legitimate accounts. For this reason, we see security mechanisms as an important safeguard to manage this risk.

4.64 Having considered the impacts, risks and benefits associated with the proposed measure, we consider it to be proportionate when assessed against its intended purpose. While there is some potential for friction and limited interference with rights, these impacts are mitigated by the safeguards proposed and are outweighed by the benefits of preventing account takeover and reducing fraudulent advertising.

4.65 Given the scale of harm prevented, the clear link between the proposed measure and its intended aim, and the flexibility afforded to service providers in selecting appropriate mechanisms, we consider that the benefits outweigh the identified costs and potential impacts. Reducing the risk of account takeover helps prevent fraudulent advertising, which in turn protects users and maintains trust in online advertising. We therefore conclude that this proposed measure represents a proportionate and justified intervention for Category 1 and 2A service providers.

4.66 The full text of the proposed measure can be found in the draft Fraudulent Advertising Code of Practice for user-to-user services and in the draft Fraudulent Advertising Code of Practice for search services, and it is referred to as FAU H3 and FAS H3 respectively.

Account takeover reporting

Explanation of the proposed measure

4.67 The proposed measure recommends that service providers implement a reporting mechanism that enables advertising account holders to report suspected account takeover.

4.68 We propose to recommend that:

a) the reporting mechanism should be easy to find, access and use; and
b) the service provider should promptly review the suspected account takeover report and take appropriate action in line with its decision. Any appropriate action should be taken swiftly.

4.69 We provide further details on how these elements apply to account takeover reporting in the following paragraphs.

4.70 We consider this proposed measure to be complementary to the proposed account security measure, which focuses on reducing the likelihood of account takeover occurring. This proposed measure is intended to limit the harm caused where an account takeover has already taken place.

Reporting mechanism that is easy to find, easy to access and easy to use

4.71 The emphasis on reporting mechanisms being easy to find, use and access aligns with the approach set out in Volume 4, Section 4, 'Advertising complaints'.

4.72 Service providers should consider these factors:

a) The reporting mechanism should be easy to find and easily accessible.
b) The reporting processes should be designed so that they only include reasonably necessary steps.
c) The advertising account holders should have the ability to provide supporting information.

d) When designing a takeover reporting mechanism, the service provider should also consider the accessibility needs of advertising account holders.

Reporting mechanism should be easy to find and easily accessible

4.73 When designing a takeover reporting mechanism, the service provider should ensure it is sufficiently prominent within the service (for instance, through its placement and visual presentation, such as the font used and how it is displayed).

4.74 The service provider should also enable the use of the reporting mechanism without requiring the advertising account holder to be logged into an account.

4.75 This is important because it allows legitimate advertising account holders who have lost access to their account, due to an account takeover, to report the problem promptly. In practice, such reporting mechanisms are likely to be accessed via a service's help centre or sign-in page, where they can be made available regardless of whether an individual is logged into an account.

4.76 Allowing reports to be submitted without being logged in helps reduce delays in reporting and mitigates the risk of ongoing harm resulting from the dissemination of fraudulent advertisements or a fraudulent advertising proxy. However, this approach could also be misused. For example, someone could submit a false report to try to take over an account. Service providers should make sure that account recovery processes are robust and prevent malicious access.

Reporting processes should only include reasonably necessary steps

4.77 Service providers should ensure that their reporting mechanism includes only those steps that are reasonably necessary to submit the report and restore the account to the legitimate holder.

4.78 Reporting processes for account takeover should be designed so that:

a) They are effective for the specific context of account takeover.
b) They use only the reasonably necessary steps needed to submit the report and, where appropriate, restore access to the legitimate account holder.
c) They avoid placing unnecessary burden on the advertising account holder.

4.79 We consider that an appropriate balance is needed between making the reporting mechanism quick and easy to use, while also ensuring that the service provider obtains the necessary information to handle reports.

4.80 What constitutes 'reasonably necessary steps' will depend on provider-specific factors and the nature of the account. These steps should not place an unnecessary burden on the person making the report, nor require information or actions that are not materially relevant to handling the account takeover.

Advertising account holders should be able to provide supporting information

4.81 The reporting process should be designed to ensure service providers are able to better understand the context of the report and make an accurate assessment before making a decision. The advertising account holder should be able to submit supporting information to supplement their report of account takeover. In practice, this could mean that service providers implement functionalities that allow the account holder to attach screenshots, insert URLs and provide additional context in free-text boxes.

Accessibility of the reporting mechanism

4.82 Service providers should also consider the accessibility needs of advertising account holders when designing the reporting mechanism. This includes consideration of:

a) the relevant information they hold about advertising account holders, including whether these users have any specific needs; and
b) industry standards and good practice on accessibility for disabled people, including implementing assistive technologies to increase the mechanisms' usability (such as keyboard navigation and screen-reading technology).

4.83 An example of accessibility when designing a takeover reporting mechanism includes using clear, plain language throughout the reporting flow so that users can easily understand each step, and ensuring the mechanism is available and easy to use on both web and mobile.[150]

4.84 For further detail see Volume 4, Section 4, 'Advertising complaints'.

Reviewing the report promptly and taking appropriate action

4.85 The service provider should promptly review the suspected account takeover report and subsequently take appropriate action in line with the decision of their review. Any appropriate action should be taken swiftly.

Reviewing

4.86 We consider it important that service providers review account takeover reports promptly, taking into account the potential for ongoing harm.

Taking appropriate action

4.87 The appropriate action the service provider takes in response to a report of account takeover should aim to minimise the risk of the compromised account posting fraudulent advertisements or a fraudulent advertising proxy.

4.88 Although we do not seek to prescribe the precise action service providers should take, we consider that appropriate action should include the following, at a minimum:

a) The provider should restore access to the legitimate account holder if they decide there has been account takeover. As part of this, the provider should satisfy itself that:
    i) it is restoring access to the legitimate account holder (given the risk of malicious reports); and
    ii) the account no longer poses a risk of being used to post fraudulent advertisements.
b) The provider should prevent the account from posting paid-for advertisements which can be encountered by UK users until the steps in point (a) have taken place.

4.89 A report of account takeover may result in a service provider deciding to withdraw a ban where an account has been found to have posted fraudulent advertisements.[151] Any such decision should only be taken where the provider has taken reasonable steps to be satisfied that the account is no longer compromised and that restoration would not present an ongoing risk of the account being used to post fraudulent advertising. The 'reasonable

[150] Ofcom research found that reporting an account takeover involved multiple steps and was not consistently signposted. This research reflects a snapshot of platform features and functionalities. Source: Ofcom, 2026. Behavioural audit of services with advertisement functionality.
[151] See Volume 3, Section 5, 'Advertising bans'.

steps' taken will depend on the service and the individual case but will likely involve reviewing information submitted as part of the account takeover report.

4.90 In some cases, restoration may not be appropriate. This may arise where the service provider cannot restore access to the account for the legitimate account holder, or the provider considers that the account may still be at risk of being used for fraudulent advertising. In such circumstances, the provider may decide to take alternative action to prevent further harm or misuse.

4.91 Further details on our proposed recommendations regarding account banning can be found in Volume 3, Section 5, 'Advertising bans'.

Submitting a report or an appeal

4.92 We are proposing to recommend that service providers allow account holders to submit account takeover reports. Service providers should normally treat an account takeover report as an appeal against a ban, but the provider should not require the account holder to follow a separate appeal process such as the one set out in Volume 3, Section 6, 'Account appeals'.

4.93 A service provider should consider account takeover reports when deciding whether to uphold or overturn a ban on an advertising account.[152]

Benefits and effectiveness

4.94 Account takeover reporting is an essential safeguard that allows service providers to act quickly if an account is taken over, helping prevent fraudulent advertisements or proxies from being published or disseminated.

4.95 Research indicates that businesses can find the process of reporting fraudulent advertisements to be cumbersome and inconsistent, and it is particularly challenging to report account takeover.[153]

4.96 Ofcom research also suggests that reporting tools are difficult for users to locate and navigate. Processes for reporting account takeover in an advertising context are not always clearly signposted and may be located within general help flows.[154]

4.97 The evidence on reporting processes points to the importance of having reporting processes in place and ensuring they meet certain standards. Account takeover is a fraud tactic that continues to present a risk, and strengthened checks may prompt further attempts. We therefore consider a robust reporting mechanism necessary.

4.98 Having regard to the components in paragraph 4.72 will make it easier for advertising account holders to report suspected account takeovers, increasing engagement with the reporting mechanism.

4.99 These steps will make it more likely that an advertising account holder is able to report suspected account takeover promptly and effectively.

[152] See Volume 3, Section 5, 'Advertising Bans'.
[153] Ofcom, 2026. Online advertising pathways: qualitative research report; Ofcom, 2026. Behavioural audit of services with advertisement functionality.
[154] Ofcom, 2026. Behavioural audit of services with advertisement functionality.

4.100 Increased reporting should enable providers to take timely action, which could include potentially recovering the account, which helps limit user exposure to fraudulent advertisements or proxies and reduces resulting harm.

4.101 The guidance we provide in paragraphs 4.87 to 4.91 on appropriate action when a service provider receives a report of account takeover helps return access to the legitimate account holder, rather than a bad actor, and reduces the risk of fraudulent advertisements being posted.

Impacts and costs on service providers

Direct costs for service providers

Implementing a mechanism to report suspected account takeovers, reviewing suspected account takeover reports and taking appropriate action

4.102 All Category 1 and 2A service providers that are in scope of this proposed measure would also be in scope of the reporting and complaints duties under the Act.[155] As mentioned in our December 2024 Statement on Protecting People from Illegal Harms Online, we consider the measure on enabling complaints for illegal content is the minimum action necessary for service providers to comply with this requirement from the Act.[156] Category 1 and 2A service providers should already have systems and processes (for example, reporting mechanisms) in place to enable complaints for illegal content, and we expect that they would be able to adapt this to provide advertising account holders with a mechanism to report suspected account takeovers.

4.103 In doing this, it is likely that the main additional input needed would be staff and engineering time to design, test and implement the adaptations needed. At a high level, providers may need to: update the reporting infrastructures to ensure advertising account holders (in addition to users) can submit reports, update the reporting interfaces and menus to include an additional category for reporting suspected account takeovers, and update existing reporting workflows to enable the storing of additional reports and ensure these reports are routed to the relevant team.

4.104 We assume that these adaptations may involve additional full-time work over a period of three to six weeks from two software engineers and one professional occupation staff member (for example, a project manager, policy manager). Based on this, we estimate a potential one-off cost of between £12,500 and £50,100.[157] Actual costs may vary by provider, depending on the extent and complexity of the adaptations needed. These costs could also be higher for providers with more complex internal processes for making changes to existing systems. In line with standard assumptions, we also estimate an annual ongoing cost of between £3,100 to £12,500 involved in maintaining the infrastructure and relevant workflows as service needs change over time.[158]

4.105 There will be other ongoing costs, mainly in relation to the cost of reviewing and processing suspected account takeover reports and subsequently taking appropriate action. This will depend on the number of reports received per year and the length of time needed to

[155] The illegal harms duties, and for services likely to be accessed by children, the protection of children duties.
[156] See ICU D1, Illegal content Codes of Practice for user-to-user services.
[157] See Annex 8, 'Further detail on economic assumptions and analysis'
[158] Our standard assumption is that maintenance (excluding any significant improvement) would be 25% of initial costs. See Annex 8, 'Further detail on economic assumptions and analysis'

review and process each report before taking an action. This is also likely to involve staff training and support tools to ensure that relevant staff can effectively and consistently review and process the reports.

4.106 Providers may choose to implement this proposed measure alongside our recommendations in Volume 4, Section 4, 'Advertising complaints', to benefit from the significant cost overlap across these proposed measures, especially in relation to the work that may be necessary in adapting the relevant reporting and complaints measure in the Illegal Content Codes of Practice. This could help reduce overall costs, especially the potential one-off costs involved across the measures.

4.107 Many Category 1 and 2A providers already offer advertisers mechanisms to report suspected account takeovers.[159] These are often embedded into the account recovery tools provided to advertising account holders. For these providers, the main additional costs will be in ensuring their reporting mechanism aligns with our recommendation on the design of the mechanism, which we consider below.

Reporting mechanism should be easy to find, access and use

4.108 When providing advertising account holders with a mechanism to report suspected account takeovers, service providers should also have regard to the proposed recommendation that the mechanism should be easy to find, access and use by advertising account holders. [160]

4.109 Providers may incur one-off costs associated with planning and implementing the necessary interface design features (this could involve undertaking research to better understand reporting needs), as well as testing and refining the design features.

4.110 We assume that providers may need full-time work over a period of two to eight weeks from one user experience designer and professional occupation staff member (for example, a researcher), and part-time involvement from one software engineer.[161] Based on this, we estimate one-off costs of between £5,600 and £44,600.[162] It is likely that costs will scale in line with the complexity of any technical changes needed to implement the necessary interface design features.

4.111 In addition to the one-off costs, there would be annual maintenance costs involved in upkeep of the interface design features and making adjustments as service needs change. We estimate these annual maintenance costs to range between £1,400 and £11,100 in line with our standard assumptions.[163] There may also be other costs in ensuring that the reporting mechanism remains easy to find, access and use over time, as advertiser needs and industry good practice change and develop. For example, providers could conduct periodic reviews to ensure their understanding remains up to date.

---

[159] For example, Google, no date. What to do if your account is compromised. [accessed 6 May 2026].
[160] In practice, we expect that service providers would consider this recommendation when implementing the reporting mechanism, which we have considered the costs for above (see paragraphs 4.102 to 4.107). We expect there would be scope to merge costs between these two components of the proposed measure.
[161] Half of a full-time equivalent of one software engineer.
[162] See Annex 8, 'Further detail on economic assumptions and analysis'.
[163] Our standard assumptions are that maintenance (excluding any significant improvement) would be 25% of initial costs. See Annex 8, 'Further detail on economic assumptions and analysis'.

4.112 Our proposed measure relating to the design of advertising complaints systems and processes also has the equivalent proposed recommendation. [164] In practice, service providers may find it cost-effective to integrate this proposed measure into the equivalent measure set out in Volume 4, Section 4, on 'Advertising complaints', to account for the significant cost overlap (for example, planning and testing out the relevant interface design features). If accounting for this overlap, service providers are likely to incur costs closer to the lower bound of our estimated ranges in the preceding paragraphs.

4.113 We also expect there to be some cost overlap with our proposed measure on enabling complaints, which similarly does not require users to be registered or have an account to make reports.[165] We are also aware that, where similar mechanisms are already provided for the purpose of account takeover reporting, service providers already often enable account holders to submit reports without being logged into an account and to submit supporting information.[166] Therefore, providers that already provide these functionalities are unlikely to incur significant additional costs.

Rights assessment

Freedom of expression and freedom of association

4.114 As explained in paragraph 4.48, we start from the position that this proposed measure is prescribed by law, in pursuit of a legitimate aim and corresponds to a pressing social need.[167]

4.115 We do not consider that the proposed recommendation for providers to have a reporting mechanism as part of this measure will have any negative impact on the right to freedom of expression for service providers, users of the service or advertisers. However, our analysis in relation to freedom of expression, freedom of association and degree of interference in paragraphs 4.48 to 4.54 applies equally in relation to the proposed recommendation that providers take appropriate action against an account holder in response to a report of account takeover. Whether an account holder is restricted from accessing their account due to failed account checks or a report of account takeover, the impact on their freedom of expression will likely be the same.

4.116 We consider that any impact on freedom of expression is likely to be limited, and the impact would predominantly affect perpetrators of fraud against whom account takeover reports are made, and we do not consider that fraudulent account takeover is protected under Article 10 of the ECHR. However, we recognise that there is a risk that legitimate advertising account holders may also be restricted from accessing their own accounts in the event of an incorrect or malicious report of account takeover. We recognise that service providers already have account recovery mechanisms in place, and we expect these arrangements to continue. This proposed measure also includes safeguards to mitigate

[164] Volume 4, Section 4, 'Advertising complaints': Having easy to find, easy to access and easy to use advertising complaints systems and processes.
[165] Volume 4, Section 4, 'Advertising complaints': Enabling Complaints.
[166] Google, no date. What to do if your account is compromised. [accessed 6 May 2026]; Microsoft, no date. How to recover a hacked or compromised Microsoft account. [accessed 6 May 2026].
[167] As also explained in paragraph 4.48 to 4.49, Article 10 of the ECHR upholds the right to freedom of expression. We must exercise our duties under the Act in a way that does not restrict this right unless satisfied that is proportionate to the legitimate aim pursued.

against this risk, including a recommendation that service providers should restore access to the legitimate account holder where viable and appropriate.

4.117 We consider that the proposed measure also has the potential to positively influence advertisers' right to freedom of expression, by implementing a mechanism through which owners of advertising accounts can report and restore access to their account in the event it is compromised. Service users' right to freedom of expression may also be indirectly positively influenced, as they would benefit from protections from fraudulent advertising, which they may otherwise have encountered on the service without the report of account takeover.

4.118 To the extent that this proposed measure will involve interference with rights to freedom of expression, we consider the interference to be proportionate to the Act's legitimate objective of protecting individuals in the UK from fraudulent advertising.

Data protection and privacy

4.119 As set out in paragraphs 4.55 to 4.60, service providers will be required to comply with data protection legislation when implementing this proposed measure. This will include publishing information about their account security mechanisms, including their account takeover reporting policy, as part of their privacy notice, as required by Articles 12 to 14 of the UK GDPR.

4.120 We recognise that publishing too much detail could assist bad actors by revealing how security mechanisms operate. We therefore expect service providers to share information at a sufficiently high level, without disclosing details that could be misused.

4.121 We recognise that this proposed measure will interfere with individuals' right to privacy as service providers will need to process the personal data of the account owner to satisfy themselves as to the account holder's identity, and their relationship to the account they are seeking to recover, as part of considering the reports of suspected account takeover.

4.122 We recognise that the level of interference with individuals' privacy will depend on how a service provider decides to implement this proposed measure. The proposed measure gives providers flexibility in how they implement reporting and what data they collect. In implementing the proposed measure, providers must comply with relevant data protection laws, and should consider relevant ICO guidance on the processing of personal data.[168]

4.123 Overall, we consider the degree of interference to privacy rights to be proportionate to the Act's legitimate objective of protecting individuals in the UK from fraudulent advertising.

Provisional conclusion

4.124 All Category 1 and 2A service providers must have in place proportionate systems and processes designed to protect users from fraudulent advertising in accordance with their duties under sections 38(1) and 39(1) of the Act. Our proposed approach is to recommend that, to enable this, service providers should implement an account takeover reporting mechanism.

[168] ICO, 2026. Automated decision-making, including profiling. [accessed 9 June 2026] [ICO guidance in draft at time of publication]; ICO, no date. Online safety and data protection. [accessed 6 May 2026].

4.125 We provisionally consider that such a measure should help to reduce harm where account takeover does occur by providing the legitimate account holder with a means to report the incident and restore access.

4.126 Our proposed recommendations on advertising account checks will increase friction for bad actors, which may in turn lead to increased attempts to gain unauthorised access to advertising accounts. In light of this, we consider the proposed reporting measure to be an important mitigation to address this potential vulnerability. An account takeover reporting mechanism would also enable account holders to notify service providers when their account has been compromised. This would support timely review and action to prevent bad actors from posting or disseminating fraudulent advertisements or fraudulent advertising proxies.

4.127 Many service providers already operate reporting mechanisms that they could adapt for this purpose. Therefore, we consider that the costs associated with enabling account takeover reporting are likely to be limited, particularly when set against the benefits it would deliver.

4.128 We see this proposed measure as a means of reducing harm by limiting the level of fraudulent advertisements and fraudulent advertising proxies encounterable by UK users. The proposed measure should enable service providers to be promptly alerted when an account has been compromised, and to take timely action to prevent further misuse. At the same time, the measure should support legitimate advertising account holders in restoring access to their accounts, where appropriate. Taken together, the effects of this proposed reporting mechanism should help disrupt bad actors.

4.129 Our provisional view is therefore that the proposed measure is proportionate for Category 1 and 2A services.

4.130 The full text of the proposed measure can be found in the draft Fraudulent Advertising Code of Practice for user-to-user services and in the draft Fraudulent Advertising Code of Practice for search services, and it is referred to as FAU H4 and FAS H4 respectively.

5. Advertising bans

What is this section about?

Advertising bans involve preventing advertising account holders that are found to have posted fraudulent advertisements from posting paid-for advertisements to UK users on the service, and taking reasonable steps to prevent banned advertising account holders from returning to the service.

In this section we set out our proposed measure for advertising bans, and why we are proposing to recommend it.

Our proposal

Number in our Codes	Proposed measure applicable to providers of Category 1 and 2A services
FAU H5 and FAS H5	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**.

Why are we proposing this?

Our proposed measure should ensure that the advertising account holders responsible for posting fraudulent advertisements are no longer able to post paid-for advertisements to UK users. This should have the benefit of reducing overall levels of fraudulent advertising, and assist providers to comply with their duties under the Act.

Consultation questions

- Do you agree with our proposal? Please provide any arguments and supporting evidence.
- Are you aware of any additional exceptional circumstances in which it may be proportionate for providers to reverse advertising bans?

Introduction

5.1 This section proposes that providers of Category 1 and Category 2A services (providers) should ban advertising account holders responsible for posting fraudulent advertisements on the service, and take reasonable steps to prevent banned advertising account holders from returning to the service. The term 'advertising account holder' refers to any person using an advertising account who is able to post paid-for advertisements.[169] This would cover both manager and individual accounts, including those with different levels of permission.

[169] See Annex 7, 'Glossary' for our definitions of 'post or posting an advertisement', 'advertising account', and 'advertising account holder'. See also Volume 1, Section 3, 'Online advertising ecosystem' for more information about the different types of persons who may use an advertising account.

5.2 For the purpose of this section, a 'ban' means to prevent an advertising account holder from posting relevant paid-for advertisements which can be encountered by United Kingdom users on the service by taking the following actions:

a) preventing the advertising account that was used to post the fraudulent advertisement or fraudulent advertising proxy[170] from being able to be used to post paid-for advertisements encounterable by UK users; and
b) taking reasonable steps to prevent the banned advertising account holder from creating and using new advertising accounts, or using existing advertising accounts to post relevant paid-for advertisements.

5.3 Where the provider bans an advertising account holder under this measure, it should also prevent the advertising account which has been used to post a fraudulent advertisement or fraudulent advertising proxy from being used to post relevant paid-for advertisements on any other Category 1 or 2A service it provides which can be accessed by that same account.

5.4 We acknowledge that a Category 1 or 2A service may be serving paid-for advertisements to its users through a range of advertising pathways. Where relevant, the proposed intermediaries measure would apply. The proposed intermediaries measure recommends the provider should use all reasonable endeavours to implement a version of any measures it has been unable to apply. For more information, see Volume 2, Section 2, 'Advertising intermediaries'.

Advertising bans

Explanation of the proposed measure

5.5 In this sub-section we explain how this measure works. We have split this explanation into the following:

a) banning advertising account holders from advertising on the service; and
b) preventing banned advertising account holders from returning to advertise on the service.

Banning advertising account holders

5.6 We propose to recommend that a service provider should ban the advertising account holders that it determines to be responsible for posting fraudulent advertisements from posting paid-for advertisements that can be encountered by UK users. The effect of an advertising ban should be that the advertising account which was used to post a fraudulent advertisement is no longer able to post paid-for advertisements that can be encountered by UK users.[171]

How service providers should ban advertising account holders

[170] A fraudulent advertising proxy is an advertisement that a service provider has assessed against its own categories of prohibited advertisements (set out in its terms of service or publicly available statement, advertising contracts (where all of the provider's advertising contracts contain similar prohibitions in relation to fraudulent advertisements), or a combination of these when read together). The provider may do this where it is satisfied that the fraudulent advertisements that it has reason to suspect exist are prohibited by these policies or contracts. For more information, see Volume 4, Section 2, 'Advertising moderation'.
[171] We are not proposing to recommend any specific actions in respect of the advertising account holder's ability to post paid-for advertisements that can be encountered by users outside the UK (or to target such users).

5.7 The Online Safety Act 2023 (the Act) is designed to protect UK users from harms online; however, we recognise that UK users may encounter paid-for advertisements posted by both UK and non-UK advertising account holders on online services. Where providers ban an advertising account holder, they should therefore prevent the advertising account that was used to post the fraudulent advertisement or fraudulent advertising proxy from being able to be used to post paid-for advertisements that can be encountered by UK users.

5.8 We expect that providers of services likely to be categorised as Category 1 and Category 2A already have the technical capability to limit the countries to which advertising accounts can target paid-for advertisements. Functionality enabling advertising accounts to target advertising campaigns by geographic location, including by country, is currently available across a range of services.[172] This often includes the ability for advertising accounts to exclude paid-for advertisements from geographic locations within a larger area.[173] Given the wide availability of this functionality, we expect that providers will be able to adapt existing location targeting functionality for the purpose of preventing banned advertising account holders from posting paid-for advertisements that can be encountered by UK users.

5.9 An advertising ban under this proposed measure applies to the posting of paid-for advertisements which may be encountered by UK users, but does not extend to other account functionalities. For example, access to the advertising account may still be required to allow the advertising account holder to carry out actions such as submitting an appeal or making payments. We understand that some providers who currently ban advertisers continue to allow account access, at least for the duration of any appeal period.[174] We discuss appeals for advertising bans in more detail in paragraphs 5.22 to 5.31.

5.10 Some services also provide functionality that allows advertising accounts to generate, upload or share user-generated content, in addition to posting paid-for advertisements.[175] A

[172] For example, LinkedIn allows advertisers to "reach member accounts based on where they live or where they live and visit using location." Advertisements may be targeted to users' permanent location, recent location or both. Source: LinkedIn, 2026. Targeting options for LinkedIn Ads. [accessed 1 May 2026]; Meta allows advertisers to "choose locations for your ad to reach people based on their country, region or city." Source: Meta, 2026. Use location targeting. [accessed 1 May 2026]; Microsoft Advertising allows advertisers to target or exclude advertising by country. Source: Microsoft, 2026. How to target customers. [accessed 1 May 2026].

[173] For example, Google Ads allows advertisers to exclude advertisements from geographic locations, including countries. Source: Google, 2026. Exclude ads from geographic locations. [accessed 16 March 2026]; Reddit allows advertisers to manually exclude specific locations including countries. Source: Reddit, 2026. Demographics. [accessed 18 March 2026]; Snapchat allows advertisers to "select specific locations to include or exclude in your targeting parameters." Source: Snap Inc., 2026. How Location Targeting Works. [accessed 1 May 2026].

[174] For example, when a Google Ads account is suspended, "all ads in the suspended account will stop running, and you will no longer be able to advertise from your suspended account until the account is reinstated." Source: Google, 2026. Google Ads account suspensions overview. [accessed 1 May 2026]; Pinterest states that, "when we remove an advertiser, they no longer have access to Pinterest's advertising tools. This doesn't affect their ability to use other Pinterest products, though." Source: Pinterest, 2025. Enforcement. [accessed 1 May 2026]; When TikTok suspends an advertising account, the advertising account can still be accessed, but all advertisements under the suspended account will be stopped, among other restrictions. Source: TikTok, 2026. About suspended ad accounts on TikTok. [accessed 1 May 2026].

[175] For example, Instagram business accounts may post both user-generated content and paid-for advertisements. Source: Meta, 2026. Set up a professional Instagram account to access business or creator tools and controls. [accessed 1 May 2026].

ban under this proposed measure only applies to the advertising account holder's ability to post paid-for advertisements to the service.[176]

How providers should determine which advertising account holders to ban

5.11 As set out in paragraph 5.2, a service provider should ban the advertising account holder that it determines to be responsible for posting a fraudulent advertisement to the service. It should do this by ensuring that the advertising account which was used to post the fraudulent advertisement is no longer able to be used to post paid-for advertisements that may be encountered by UK users. In some cases, the provider may determine that an individual advertising account holder or several advertising account holders are responsible.

5.12 The advertising account holder that the provider determines to be responsible for posting a fraudulent advertisement may vary depending on the circumstances. Advertisers may have multiple advertising accounts within their overall advertising account hierarchy, including accounts with varying levels of permissions and control over other accounts.[177] [178] An advertising account hierarchy could also include third parties such as advertising agencies that are contracted to carry out certain tasks, such as managing individual advertising campaigns.

5.13 Under this proposed measure, the advertising account holder that the provider determines to be responsible for posting a fraudulent advertisement may be a group of people.[179] Evidence indicates that the distribution of fraudulent advertisements can be coordinated by criminal operations that deploy extensive networks of accounts, as set out in Volume 1, Section 4, 'Causes and impacts of fraudulent advertising', paragraph 4.28. Additional evidence suggests that overseas scam compounds may target fraudulent advertisements to UK users.[180] In such cases, providers may determine that the advertising account holder to be banned is an organised crime group or other criminal operation, and should ban the account used to post a fraudulent advertisement, and take reasonable steps to prevent the advertising account holder from creating and using new advertising accounts, or using existing advertising accounts.

5.14 Evidence shows that under their current practices, service providers make decisions about which accounts within a hierarchy are responsible for posting fraudulent advertisements,

---

[176] The fraudulent advertising duties set out in sections 38 and 39 of the Act only extend to the systems and processes that a provider operates to protect individuals from fraudulent advertisements. Preventing advertising accounts that have posted fraudulent advertisements from posting user-generated content would not support compliance with the fraudulent advertising duties. Where accounts post fraudulent user-generated content, this is covered by the user sanctions measure proposed in our June 2025 Additional Safety Measures Consultation.

[177] We use the term 'advertising account hierarchy' to refer to multiple advertising accounts that are arranged within a structure on the service. There may be different types of advertising accounts within an advertising account hierarchy, such as 'individual' and 'manager' accounts. For more detail on these types of accounts, see Volume 1, Section 3, 'Online advertising ecosystem', paragraphs 3.19 to 3.20.

[178] For example, Microsoft Advertising allows multiple manager and non-manager accounts to be linked together across an advertising account hierarchy. Source: Microsoft, 2026. Hierarchies in Microsoft Advertising. [accessed 26 March 2026].

[179] In accordance with Section 236 of the Online Safety Act 2023, which provides that a 'person' includes (in addition to an individual and a body of persons corporate or unincorporate) any organisation or association of persons.

[180] National Crime Agency, 2026. Fraudsters arrested in Nigeria following NCA intelligence sharing. [accessed 25 June 2026].

and apply bans and other account restrictions in accordance with those decisions.[181] We recognise that this practice enables providers to apply bans to more effectively prevent fraudulent advertising.

5.15 In some cases, the service provider may find advertising accounts that do not sit within the advertising account hierarchy, but that it suspects are also operated or managed by the advertising account holder responsible for posting a fraudulent advertisement. Where this occurs, providers should take appropriate action against these advertising account holders as a reasonable step to prevent return. The types of action that we expect that providers take against such advertising account holders includes bans, account checks, and account restrictions.[182] We describe these actions in more detail in paragraphs 5.32 to 5.45.

Application of bans where an advertising account can advertise across multiple services

5.16 Some providers of Category 1 and Category 2A services offer functionality that allows a single advertising account to access and post paid-for advertisements across multiple services.[183] This can have benefits for advertisers, such as allowing one advertising account to manage advertising campaigns across multiple services.

5.17 Service providers can also use this functionality to implement restrictions for one advertising account across multiple services. On some providers' advertising networks, account restrictions are already applied across multiple services.[184] Where a provider applies restrictions such as bans or suspensions on posting paid-for advertisements at the account level, this prevents the advertising account from posting paid-for advertisements on the multiple services that it has access to.

5.18 We propose that, where the provider bans an advertising account holder, it should also prevent the advertising account used to post a fraudulent advertisement from being used to post paid-for advertisements on any other Category 1 or Category 2A service it provides, where the same advertising account can be used to post paid-for advertisements across those services. This is relevant where a provider operates multiple Category 1 or Category 2A services, and there is functionality for a single advertising account to access those multiple services and post paid-for advertisements on them.[185] Where an advertising account holder posts a fraudulent advertisement on one of the services belonging to the provider, there is the risk that the advertising account holder may post fraudulent advertisements on the other services that the advertising account can access. We consider

---

[181] For example, Meta states that it may apply advertising restrictions to multiple types of accounts with advertising functionality, such as business portfolios, advertising accounts, Facebook Pages and user accounts. Individual user accounts that are attached to business portfolios, advertising accounts or Pages may be restricted without the restrictions applying to other user accounts attached to these assets. Source: Meta, 2026. About advertising restrictions. [accessed 26 March 2026].

[182] For more details of our proposals on account checks and account restrictions, see Volume 3, Section 2, 'Account checks and actions'.

[183] For example, Google Ads accounts can post advertisements across the Google Network, including Google Search and YouTube. Source: Google, 2026. Google Network. [accessed 18 March 2026]; Meta Ads Manager allows advertising accounts to post advertisements on Facebook, Instagram, Messenger and Audience Network. Source: Meta, 2026. Facebook Ads Manager. [accessed 18 March 2026].

[184] For example, Meta states that advertising account restrictions apply across Meta technologies. Source: Meta, 2026. Introduction to the Advertising Standards. [accessed 18 March 2026].

[185] Our proposed recommendation applies to services in scope of the fraudulent advertising duties. Service providers may still choose to apply restrictions or bans to advertising accounts where they can also post paid-for advertisements on services not in scope of the duties.

that this would pose an unacceptably high risk to the UK users of those other services if the ban were limited only to the service on which fraudulent advertisements were posted.

How this proposed measure applies to both fraudulent advertisements and fraudulent advertising proxy

5.19 When applying this proposed measure, service providers may choose to remove fraudulent advertisements in accordance with their terms of service or publicly available statements without necessarily making a fraudulent advertising judgement.[186] We are therefore proposing to recommend that this measure applies to advertising account holders that post either fraudulent advertisements or fraudulent advertising proxy.

5.20 As set out in Volume 4, Section 2, 'Advertising moderation', paragraphs 2.10 and 2.11, fraudulent advertising proxy is defined as an advertisement that the service provider has assessed against its own categories of prohibited advertisements rather than making a fraudulent advertisement judgement per the draft guidance on fraudulent advertising judgements. The provider may do this where it is satisfied the types of content included in these policies or contracts are broad enough to cover the fraudulent advertisements that it has reason to suspect exist. We consider that providers are unlikely to use broad proxies which capture types of advertising that are highly unlikely to be fraudulent, unless they have made a commercial decision to do so.

5.21 Where this section refers to fraudulent advertisements, this therefore includes both fraudulent advertisements and fraudulent advertising proxy, unless otherwise specified.

Appeals

Considering appeals where paid-for advertisements have been incorrectly identified as fraudulent advertisements

5.22 We propose to recommend that advertising account holders should be able to submit advertising appeals where they consider that they have received a ban as the result of a paid-for advertisement being incorrectly judged to be a fraudulent advertisement.

5.23 Service providers should deal with such appeals by following the steps we propose in Volume 4, Section 4, 'Advertising complaints', sub-section 'Appropriate action for advertising complaints which are advertising appeals'. There we propose to recommend that, where an advertising appeal is upheld and a provider reverses a decision that a paid-for advertisement was a fraudulent advertisement, the provider should, so far as appropriate and possible, reverse the action taken against the paid-for advertisement and the advertising account holder to restore their original position had the decision not been made.

Considering appeals in relation to the placement of a ban

5.24 We propose to recommend that advertising account holders should be able to use the account appeals process set out in Volume 3, Section 6, 'Account appeals' to dispute an advertising ban where they believe it has been applied to the wrong advertising account holder. Where the appeal is upheld, the provider should assess whether an advertising ban would be more appropriately applied to other advertising account holders in connection with the fraudulent advertisements posted. Where this is the case, the provider should reverse the original decision to impose the advertising ban on the affected advertising

[186] See Annex 11, 'Draft annex to ICJG – Guidance on fraudulent advertising judgements'.

account holder, and instead impose the advertising ban on those advertising account holders identified as more appropriate.

Considering appeals in relation to account takeover

5.25 As set out in Volume 3, Section 4, 'Countering account takeover', bad actors may seek to take control of other advertising accounts to disseminate fraudulent advertisements. We understand that this is typically responsible for [✂] of fraudulent advertising but represents a material and foreseeable risk to advertisers.[187]

5.26 A report of account takeover may result in a service provider deciding to reverse a ban where a compromised account has been found to have posted a fraudulent advertisement. Any such decision should only be taken where the provider has taken reasonable steps to be satisfied that the account is no longer compromised and that restoration would not present an ongoing risk of the account being used to post fraudulent advertisements.

5.27 In some cases, restoration may not be appropriate. This may arise where the service provider cannot confidently restore access to the account for the legitimate advertising account holder, or the provider considers that the account may still be at risk of being used for fraudulent advertising. In such circumstances, the provider may decide to take alternative action to prevent further harm or misuse.

5.28 Further details on our proposed recommendations regarding account takeover can be found in Volume 3, Section 4, 'Countering account takeover'.

Circumstances where bans may be reversed where a paid-for advertisement has correctly been identified as a fraudulent advertisement

5.29 When developing this proposed measure, we considered whether there are other exceptional circumstances in which bans should be reversed even though the paid-for advertisement has correctly been identified as a fraudulent advertisement. We have not identified evidence of any other kinds of exceptional circumstances occurring in addition to the circumstances specified in paragraph 5.24 and paragraphs 5.25 to 5.28.

5.30 We therefore propose to recommend that, where a paid-for advertisement has been correctly identified as a fraudulent advertisement, appeals will only be allowed in the following circumstances:

a) where the appeal relates to which advertising account holder has been banned; or
b) where the account has been taken over.

5.31 We would welcome evidence from stakeholders about any other exceptional circumstances in which it may be proportionate for service providers to reverse bans.

[187] We understand that the proportion of fraudulent advertisements detected and originating from compromised accounts, in a given year, was around [✂] to [✂] and [✂]. Source: [✂] response to our formal information request issued 30 January 2026; [✂] response to our formal information request issued 30 January 2026; [✂] response to our formal information request issued 30 January 2026; [✂] response to our formal information request issued 30 January 2026; [✂] response to our formal information request issued 30 January 2026; and [✂] response to our formal information request issued 30 January 2026.

Preventing return

5.32 We propose to recommend that service providers should take reasonable steps to prevent banned advertising account holders from posting paid-for advertisements that can be encountered by UK users through:

a) the creation and use by the banned advertising account holder of new advertising accounts that can place advertisements that are able to be encountered by UK users on the service; and
b) the use by the banned advertising account holder of existing advertising accounts that can place advertisements that are able to be encountered by UK users on the service.

5.33 The steps providers take should materially reduce the ability of banned advertising account holders to post paid-for advertisements that can be encountered by UK users on the service. In accordance with our proposed account checks and actions measure, providers should record in their account checks and actions policy the account checks and restrictions that would enable them to meet this objective. [188]

5.34 For the remainder of this section, we use the term 'return' to refer to where a banned advertising account holder is able to circumvent the ban by using advertising accounts to post paid-for advertisements that can be encountered by UK users.

How banned advertising account holders may return to a service

5.35 In Volume 1, Section 4, 'Causes and impacts of fraudulent advertising', we set out that banned advertising account holders may attempt to return to a service through several methods, including:

a) creating new advertising accounts (sometimes referred to as 'phoenixing');[189]
b) using other advertising accounts that already exist on the service (sometimes referred to as 'lifeboating');[190] or
c) taking over accounts that belong to other advertising account holders.[191]

5.36 In the following sub-section we set out the steps that providers should take to prevent return via the creation of new advertising accounts and the use of existing accounts. We cover account takeover, and the steps that we propose to recommend that service providers take to prevent it, in Volume 3, Section 4, 'Countering account takeover'.

How providers should prevent return

5.37 The reasonable steps that service providers take to prevent return should include:

a) undertaking checks to ensure that those seeking to open new accounts are not subject to a ban; and
b) taking action to prevent return via existing accounts.

5.38 In addition to the steps recommended under this measure, service providers should consider how the findings of their fraud indicator assessment (or equivalent) can inform the

---

[188] See Volume 3, Section 2, 'Account checks and actions', sub-section 'Development, regular review and update of the policy' and Volume 3, Section 2, 'Account checks and actions', paragraph 2.45 for more detail on our proposals on record-keeping in relation to account checks and account restrictions respectively.
[189] Volume 1, Section 4, 'Causes and impacts of fraudulent advertising', paragraph 4.29].
[190] [Ibid., paragraph 4.29].
[191] See, for example, X's policy on authenticity, which prohibits the evasion of enforcement actions taken by X, and sets out the methods by which this may occur. Source: X, 2025. Authenticity. [accessed 30 April 2026].

steps that they take to prevent return.[192] Understanding the characteristics of advertising accounts banned for posting fraudulent advertisements can help providers find advertising accounts that are being used by banned advertising account holders that share similar patterns.

5.39 Fraud is an adversarial space, and bad actors will attempt to bypass the steps taken by service providers to prevent return. However, we expect that the reasonable steps that providers take under this proposed measure should have the result of materially reducing the ability of bad actors to return to the service following a ban. What is 'reasonable' may vary by provider, taking into account matters such as the nature and functionality of the service, its available resources, and what is technically feasible.

Actions providers should take to prevent return

5.40 Providers should take reasonable steps to prevent banned advertising account holders from creating and using new advertising accounts, or from using existing advertising accounts to post paid-for advertisements.

5.41 Providers should seek to identify advertising accounts which may be being used by the banned advertising account holder. Providers should also carry out account checks during account creation and onboarding in accordance with the proposals set out in Volume 3, Section 2, 'Account checks and actions', sub-section 'Checks that providers carry out to prevent banned advertising account holders returning'.[193]

5.42 Other actions that service providers could take to look for accounts being used by banned advertising account holders include:

- using information from advertising moderation on the service to identify similarities in behaviour between advertising accounts (for example, where an account posts paid-for advertisements that match paid-for advertisements previously posted by a banned account, this may indicate that the account is being used by a banned advertising account holder);
- the use of proactive technology to find suspicious paid-for advertisements and accounts that may be being used by banned advertising account holders; [194]
- using information from external sources such as trusted flagger reports to identify accounts that are being used by banned advertising account holders.

5.43 Where a provider has reason to suspect that an existing account is being used by a banned advertising account holder, they should carry out repeat checks against the account, in accordance with the proposed account checks and actions measure. Details of our proposal

---

[192] Volume 2, Section 3, 'Fraud indicator assessment'.

[193] Evidence indicates that service providers already take steps to identify accounts being used by banned advertising account holders. For example, [✂] stated that "Where an account is disabled, we use a combination of human and automated review to prevent that individual from setting up a new account. A large proportion of this [✂] we detect connections to previously problematic or disabled accounts using indicators such as account names, registration details, and content." Source: [✂] response to our formal information request issued 30 January 2026. [✂] Source: [✂] response to our formal information request issued 30 January 2026.

[194] We understand that many large service providers use proactive technology to detect fraudulent advertisements and we plan to propose measures on this in Autumn 2026. See Volume 4, Section 2, 'Advertising moderation', paragraphs 2.14 and 2.15 for more detail.

on repeat checks can be seen in full in Volume 3, Section 2, 'Account checks and actions' sub-section 'Repeat checks and existing accounts'.

5.44 Where a provider determines that an advertising account is being used by a banned advertising account holder, the provider should ban that account, preventing it from being used to post paid-for advertisements. If a provider has reason to suspect that an account is being used by a banned advertising account holder but cannot make a determination, the provider should apply a restriction to the account as set out at Volume 3, Section 2, 'Account checks and actions', sub-section 'Applying restrictions to advertising accounts with a risk that they will post fraudulent advertising', in order to mitigate the risk of the account being used to post fraudulent advertisements. The restriction imposed by the provider should appropriately reflect the level of suspicion against the account being used by a banned advertising account holder, and the level of risk presented by the account of being used to post fraudulent advertisements.

5.45 Providers should record details of their policy on account checks at onboarding, repeat checks carried out on existing accounts, and restrictions to be placed on accounts in accordance with the proposed account checks and actions measure. Further information on record-keeping in accordance with the account checks measure can be found in Volume 3, Section 2, 'Account checks and actions', sub-section 'Development, regular review and update of the policy' and Volume 3, Section 2, 'Account checks and actions', paragraph 2.45.

Benefits and effectiveness

5.46 This proposed measure will contribute to reducing fraudulent advertising principally by ensuring that service providers take effective action at the account level when they detect fraudulent activity. Advertising bans reinforce the benefits of advertising moderation by ensuring that, alongside fraudulent advertisements being taken down, the advertising account holders responsible for posting fraudulent advertisements are no longer able to post paid-for advertisements to UK users on the service. This should have the benefit of reducing fraudulent advertising at scale when implemented on a service-wide level.

5.47 Many service providers currently apply a range of sanctions in relation to advertising accounts that violate their advertising rules, ranging from warnings and strikes, to advertising restrictions, suspensions and bans.[195] Our view is that sanctions policies of the kind currently operated by providers are less effective than advertising bans in preventing users from encountering fraudulent advertisements. Sanctions policies that escalate over time in response to repeat violations give bad actors the opportunity to post fraudulent advertisements on multiple occasions before providers take robust action at the account level. In some cases, advertising accounts may accumulate large numbers of strikes before

[195] Google stated that if an advertiser violates a Google Ads policy, Google sends a warning outlining the nature of the policy violation, giving the advertiser an opportunity to remedy the violation or explain why they believe they have not violated the policy. If this is not remedied, Google will issue suspensions according to a progressive strike system. For egregious policy violation, Google suspends the account immediately without prior warning. Source: Google response to our formal information request issued 30 January 2026.

being prevented from posting paid-for advertisements.[196] [197] Our proposals would extend the action that providers already take in relation to the most serious or repeat offenders, applying it to all advertising accounts that have posted a fraudulent advertisement. We consider that this will have significant benefits in reducing levels of fraudulent advertising.

5.48 As set out in Volume 1, Section 4, 'Causes and impacts of fraudulent advertising', paragraph 4.28, fraudulent advertising can be carried out by organised criminal operations. Organised groups of this nature, who set up advertising accounts for the sole purpose of distributing fraudulent advertisements, are unlikely to be deterred from posting fraudulent advertisements by sanctions such as strikes or account restrictions.[198] As research shows that these accounts can be responsible for a significant proportion of the overall volume of fraudulent advertisements on services, we consider that banning these accounts will have significant benefits for users.[199]

5.49 Given the severity of harm from fraudulent advertising,[200] we consider that fraudulent advertising can be most effectively addressed through banning advertising account holders. We recognise that one argument in favour of a sanctions-based approach is that this would give flexibility to service providers to target stricter sanctions or bans at the most serious or repeat offenders, while warnings and strikes could be used for less serious instances. However, we consider that there are limited circumstances where it is necessary for providers to be flexible in the approach that they take in relation to advertising account holders that post fraudulent advertisements, and so bans remain the most effective approach. We consider that the proposed appeals measures discussed in paragraphs 5.22 to 5.31 would account for the circumstances where it is necessary for providers to be flexible in relation to advertising account holders that post fraudulent advertisements.

5.50 The effectiveness of advertising bans is also dependent on how easily bad actors can evade them through the creation of new advertising accounts and the use of existing advertising accounts.[201] The measure proposed in this section is designed to combat these risks. If introduced, it would make it harder for fraudsters to circumvent bans, thereby delivering significant benefits.

---

[196] "A small advertiser would have to get flagged for promoting financial fraud at least eight times before Meta blocked it, a 2024 document stated. Some bigger spenders – known as 'High Value Accounts' – could accrue more than 500 strikes without Meta shutting them down, other documents say." Source: Horwitz, J., 2025. Meta is earning a fortune on a deluge of fraudulent ads, documents show, Reuters, 6 November. [accessed 26 March 2026].

[197] Evidence from the Integrity Institute indicates that strikes do not often lead to deactivation or a ban for advertising accounts, and that accounts may remain on services even after posting 15 pieces of fraudulent content. Source: Ofcom and Integrity Institute, 2026. Fraudulent advertising and account integrity: Expert insights on best practice.

[198] In its response to our June 2025 Consultation, Which? said, in relation to our proposed user sanctions measure, that the majority of fraudulent advertising is "carried out primarily by organised criminal groups who are financially motivated", and that "we do not believe that warnings will be effective for people whose full-time job is to defraud consumers." Source: Which? response to the June 2025 Consultation, p.15.

[199] Gen Digital (Corrons, L., Karabeyli, E., Khmelnytskyi, D., Bühler, T. and Pachilakis, M.), 2026. The Scam Ad Machine. [accessed 3 March 2026].

[200] Volume 1, Section 4, 'Causes and impacts of fraudulent advertising', sub-section 'Impact of fraudulent advertising'.

[201] Evidence from the Financial Conduct Authority (FCA) indicates that banned bad actors often return using new accounts or other existing accounts, and that to be effective, bans need to be combined with robust controls to prevent recidivism. Source: FCA written response dated 10 December 2025 to Ofcom informal request for information dated 25 November 2025.

5.51 In light of the analysis in this sub-section, we consider that the proposed measure would be an effective means of tackling fraudulent advertising. Given the harm caused by fraudulent advertising, our provisional view is that the benefits would be significant.

Impacts and costs on service providers

Direct costs for service providers

5.52 We expect the direct costs associated with this proposed measure to be limited. Much of the activity required to implement advertising bans sits within other proposed measures, specifically the systems used to detect fraudulent advertisements and the mechanisms for handling appeals, and the account checks and action measure.

5.53 We consider that the most straightforward ways for service providers to implement this proposed measure would be either to remove the advertising account, or to ensure that paid-for advertisements posted by a banned account cannot be encountered by UK users.

5.54 Where providers use outputs from other proposed measures to prevent return, much of the activity required to implement these steps sits within the other proposed measures, although providers would need to take additional actions to use these steps for the additional purpose of preventing return.

5.55 Providers of integrated ('walled garden') services commonly provide functionality for advertisers to target advertising campaigns to users by geographical location, including the ability to both target advertising to certain locations, and to exclude certain locations from targeting. We expect that providers could adapt their existing platform so that it could be used to implement a location-based advertiser ban by automatically adding the UK to the list of excluded geolocations. This would likely require changes to the provider's advertising campaign suite, and the development of a mechanism to manage this type of ban, through managing a list of blocked geolocations for banned advertising accounts.

5.56 As we expect that providers will generally be able to adapt existing targeting infrastructure to prevent banned accounts from posting paid-for advertisements that can be encountered by UK users, we do not consider it appropriate to seek to quantify costs associated with developing such infrastructure.

5.57 We recognise that there is likely to be significant variation in providers' existing targeting systems, including the granularity of targeting available, and that providers would need to make changes or adjustments to comply with this proposed measure. The costs of these adaptations are therefore likely to vary across providers depending on their existing systems, the scope of the changes required, and their internal processes. Due to the diverse range of services involved and the differing adjustments providers may need to undertake, we do not consider it appropriate to provide detailed estimates of these costs.

5.58 If service providers choose to implement the proposed measure by removing the advertising account, they would incur costs associated with blocking the account's ability to post paid-for advertisements, removing existing paid-for advertisements from that account, and, where appropriate, engaging with the advertising account holder. We consider these costs are likely to be limited, as providers would generally already have user or account management systems in place that support account restriction or removal. Smaller providers may be able to implement this manually with limited additional infrastructure costs, while larger providers may incur greater costs where they choose to implement more sophisticated or automated banning methods.

5.59 We address the costs of appeals processes referenced in this proposed measure in Volume 3, Section 4, 'Countering account takeover' and Section 6, 'Account Appeals', and Volume 4, Section 4, 'Advertising complaints'.

5.60 There will also be some costs associated with the steps providers take to prevent banned advertising account holders from returning to the service. We address the costs of checks to prevent return through the creation of new accounts in Volume 3, Section 2, 'Account checks and actions', sub-section 'Impacts and costs on service providers'. In relation to preventing return through existing accounts, providers may incur some costs in taking reasonable steps to identify advertising accounts potentially being used by a banned account holder following a ban. Providers may also incur some additional costs where they take further action to find, and take action against, existing accounts being used by banned advertising account holders. However, much of the activity involved in doing so is likely to sit within other proposed measures, such as advertising moderation and the use of trusted flagger reports under the proposed dedicated reporting channels measure,[202] which providers would use as inputs for this purpose. We therefore expect any additional costs of using those outputs to prevent return to be low relative to the costs of the relevant measures themselves.

5.61 The benefits of advertising bans are likely to accrue over time as repeat offending is prevented. The balance of costs and benefits therefore supports the conclusion that the proposed measure is proportionate and justified.

Indirect costs to service providers

5.62 Compared with having a sanctions policy that escalates over time, and under which some advertising account holders that received a sanction would go on to post further legitimate paid-for advertisements, there may be some lost revenue under our proposed measure. As set out in paragraphs 5.47 to 5.50, there is evidence that sanctions policies give bad actors the opportunity to post fraudulent advertisements on multiple occasions before providers stop the account from advertising to UK users. Overall, we therefore consider that any costs are justified by the benefits to users from bad actors being prevented from posting fraudulent advertisements.

5.63 Banning advertising account holders that have posted fraudulent advertisements means that service providers will no longer generate revenue from the advertisements that these advertisers post. However, we do not consider this to represent a material economic cost. Revenue derived from fraudulent advertising is not legitimate economic value.

5.64 Service providers have a certain number of advertisements they can sell. Removing fraudulent advertisements does not reduce the overall supply of available advertising space. While preventing bad actors from advertising may lead to lower prices for paid-for advertisements due to decreased demand, we do not consider this to represent a material economic loss. Evidence suggests that fraudulent advertising represents only a small proportion of total advertising so we consider any effect on price is likely to be marginal.[203]

---

[202] Volume 4, Section 4, 'Advertising complaints', sub-section 'Dedicated reporting channels for trusted flaggers to report fraudulent advertisements'.

[203] We are aware that the incidence of ad impressions suspended or taken down as a result of being fraudulent typically lies between 0% and 2% on online services. This varies from [✂], [✂], [✂], [✂], [✂], [✂], [✂], and [✂]. Sources: [✂] response to our formal information request issued 26 June 2025; [✂] response to our formal information request issued 26 June 2025; [✂] response to our formal information request issued 26

5.65 Because banned advertising account holders may appeal decisions, service providers may incur small additional costs associated with handling these appeals. These could include the systems and processes for identifying fraudulent advertisements, set out in Volume 4, Section 2, 'Advertising moderation' and the appeals processes set out in Volume 3, Section 4, 'Countering account takeover' and Section 6, 'Account Appeals', and Volume 4, Section 4, 'Advertising complaints'.

Rights assessment

Freedom of expression and freedom of association

5.66 As set out in Volume 1, Section 5, 'Approach to Codes', sub-section 'Approach to human rights assessments', Article 10 of the European Convention on Human Rights (ECHR) upholds the right to freedom of expression, which encompasses the right to hold opinions and to receive and impart information and ideas without unnecessary interference by a public authority. Article 10 is a qualified right, and we must exercise our duties under the Act in a way that does not restrict this right unless satisfied that is proportionate to the legitimate aim pursued.

5.67 As noted in Volume 1, Section 5, 'Approach to Codes', we start from the position that this proposed measure is prescribed by law, in pursuit of a legitimate aim and corresponds to a pressing social need.

5.68 We recognise that the proposed measure has the ability to interfere with an advertiser's right to freedom of expression as banning an advertising account from a service will affect both the advertising account holder's, and the ultimate advertiser's, ability to impart information to UK users through posting paid-for advertisements. There will also be an interference with UK users' freedom of expression where the proposed measure interferes with their ability to receive information from advertisers who are subject to a ban or have a restriction placed on them in order to prevent the banned person setting up a new account or using an existing one.

5.69 We also recognise that this proposed measure may interfere with providers' right to freedom of expression, as we are proposing to recommend that they ban certain advertisers from their service(s). However, our proposed measure recommends only that providers ban advertising account holders which the provider has determined to be responsible for posting fraudulent advertisements or fraudulent advertising proxy, including taking reasonable steps to prevent return, which depend on the level of suspicion the provider has about whether the account being set up, or the existing account, is being used by the banned person.

5.70 We consider it unlikely that a ban under this proposed measure would materially interfere with advertising account holders' right to freedom of association under Article 11 of the ECHR. Any interference would only arise where the advertising account holder is an individual, as opposed to representing (or purporting to represent) a business. Further, a ban under this proposed measure does not recommend that the advertising account is fully removed from accessing the service, but is only prevented from posting paid-for advertisements to UK users. Where the advertising account has access to other parts of the

June 2025; [✂] response to our formal information request issued 26 June 2025; [✂] response to our formal information request issued 24 November 2025; [✂] response to our formal information request issued 24 November 2025; [✂] response to our formal information request issued 26 June 2025.

service, such as user-to-user functionalities, under our proposed measure, the advertising ban should not prevent them from accessing this.

5.71 As referenced in Volume 4, Section 2, 'Advertising moderation', we recognise that some service providers will choose to apply this proposed measure by employing a fraudulent advertising proxy, rather than making a fraudulent advertising judgement. We expect that providers will have commercial incentives to employ a proxy which is sufficiently narrow so as not to disproportionately moderate paid-for advertisements, or ban advertising account holders as a result.

5.72 We also recognise that the potential impacts on freedom of expression and freedom of association arising from this proposed measure may result in accounts being banned from services on which they have not been found to have posted fraudulent advertisements. As set out in paragraphs 5.16 to 5.18, this will apply where an advertising account is banned across Category 1 and Category 2A services run by the same service provider, where that same account can be used to post paid-for advertisements across multiple platforms. Although the service provider would be banning the account across multiple services, we expect the ban to still only apply to one account. Although a ban which applies across multiple services will arguably present more of an interference with advertisers' and users' rights, we consider this is proportionate as the account being banned will have been found to have posted fraudulent advertisements and poses a high risk of posting further fraudulent advertisements on the other services relating to the account.

5.73 We recognise that, while the proposed measure is intended to target accounts posting fraudulent advertisements, there is a risk of false positives being identified, resulting in an advertising account holder being banned where they have not posted fraudulent advertisements or fraudulent advertising proxy. The proposed advertising bans measure also recommends that providers implement a method of appeal against a ban. We consider that these proposed advertising moderation and appeals measures provide sufficient safeguards for both freedom of expression and freedom of association.

5.74 We understand that many large service providers use proactive technology to detect fraudulent advertisements. As referenced in Volume 4, Section 2, 'Advertising moderation', we plan to propose measures on this in autumn 2026. We recognise that these proactive technology proposals may have an impact on rights relevant to this proposed banning measure, where an advertising account holder is banned as a result of fraudulent advertisements detected through the use of proactive technology. We will assess the rights impact of the proposed proactive technology measures as part of our autumn 2026 consultation.

5.75 Fraudulent advertising presents a significant risk of harm, and can have a significant adverse impact on individuals in the UK. See Volume 1, Section 4, 'Causes and impacts of fraudulent advertising', where we have set out this evidence in further detail.

5.76 We acknowledge that some of the fraudulent advertising offences as set out at section 40 of the Act are strict liability offences, and do not take into account the intent behind the offence.[204] This may therefore result in an account being banned for a 'technical breach of

[204] Among these strict liability offences is an offence under section 25 of the Financial Services and Markets Act 2000 regarding contravention of restrictions on financial promotion. See Volume 3, Section 3, 'Preventing fraudulent financial services advertising' for more information on the proposed measure in relation to financial services advertisements.

the rules', which may result in less loss or harm arising from the posting of the relevant advertisement. However, strict liability offences are still relevant fraud offences under section 40 of the Act, and are important offences which this proposed measure is designed to address. We consider that a ban implemented as a result of any offence under section 40 of the Act will be proportionate and important in tackling the ecosystem of fraudulent activity online.

5.77 We have considered whether a sanctions-based approach would be appropriate to address the harm of fraudulent advertising. That kind of approach is less likely to interfere with freedom of expression (or to a lesser extent) than a banning measure. However, for the reasons set out in paragraphs 5.46 to 5.51, we consider that sanctions short of banning advertising accounts that post fraudulent advertisements will not be sufficiently effective at addressing the harm to UK users from encountering fraudulent advertisements, and on that basis we do not think that there is a less intrusive means of achieving the intended objective.

5.78 Therefore, to the extent that this proposed measure would interfere with users' and advertisers' rights to freedom of expression and freedom of association, we consider the interference to be proportionate to the Act's legitimate objective of protecting individuals in the UK from fraudulent advertisements, which this proposed measure is intended to help providers of Category 1 and 2A services to secure.

Data protection and privacy

5.79 As explained in Volume 1, Section 5, 'Approach to Codes', Article 8 of the ECHR confers the right to respect for an individual's private and family life. Article 8 is a qualified right, and we must exercise our duties under the Act in a way that does not restrict this right unless satisfied that is proportionate to the legitimate aim pursued. As noted in relation to freedom of expression, we start from the position that this proposed measure is prescribed by law, in pursuit of a legitimate aim and corresponds to a pressing social need. Article 8 underpins the data protection laws with which service providers must comply.

5.80 We recognise that the proposed measure is likely to interfere with individuals' rights to privacy as implementing a ban on an advertising account, taking steps to prevent return and considering appeals is likely to involve service providers processing personal data relating to the individual people or data subjects who are the holders of the advertising account. In some cases, this could include special category data, such as biometric data, dependent on the methods a provider chooses to implement identity checks or to carry out further checks.

5.81 We also recognise that further processing of information will likely be required where a service provider must take steps to identify whether the banned account can post paid-for advertisements across any other Category 1 or Category 2A services owned by the provider, and take steps to ban the account from those services also. However, as this will relate to the same advertising account, any additional processing of information required to implement the ban across services should be limited.

5.82 Service providers will be required to comply with data protection law when implementing this proposed measure, including following the principles of fairness, transparency and data minimisation. We do not expect providers to gather or process more information than is necessary for the implementation of this proposed measure. Providers should also be transparent in how advertisers may be subject to a ban or sanctions and how their personal data is used for this purpose. Providers should also consider appropriate Information Commissioner's Office (ICO) guidance when implementing this proposed measure. The ICO has a range of data protection compliance guidance which we encourage providers to

consult. Of particular relevance to implementing this proposed measure is the ICO's guidance on online safety and data protection.[205]

5.83 Where a ban is applied due to an automated advertising moderation decision, this may engage data protection law on solely automated decisions with legal or similarly significant effects.[206] The UK General Data Protection Regulation places a specific restriction on making decisions based solely on automated processing of personal data, where the decision has legal or similarly significant effects. So-called automated decision-making is only permitted where service providers have implemented certain safeguards for the data subject's rights, freedoms and legitimate interests. The ICO has provided guidance on these matters.[207]

5.84 We are satisfied that this proposed measure can be implemented in accordance with data protection law. We consider that the safeguards under data protection law, as explained in paragraphs 1.84 to 1.85 and in the various pieces of ICO guidance relevant to this proposed measure, will help ensure that the impact of automated processing on data protection rights is minimised.

5.85 To the extent that this proposed measure involves interference with individuals' rights to privacy, we consider the interference to be proportionate to the Act's legitimate objective of protecting individuals in the UK from fraudulent advertising, which this proposed measure is intended to help providers of Category 1 and 2A services to secure.

Provisional conclusion

5.86 All Category 1 and 2A service providers must have in place proportionate systems and processes designed to protect users from fraudulent advertising in accordance with their duties under sections 38(1) and 39(1) of the Act. Our proposed approach is to recommend that, to enable this, all such providers ban advertising account holders that have been determined to have posted fraudulent advertisements from posting paid-for advertisements to the service, and take reasonable steps to prevent their return.

5.87 We provisionally consider that this proposed measure would likely result in fewer users being exposed to fraudulent advertising than would otherwise be the case. Applying advertising bans to advertising account holders that have posted fraudulent advertisements will prevent them from disseminating more fraudulent advertisements to users, which is likely to reduce overall levels of fraudulent advertisements on the service. Taking steps to prevent banned advertising account holders from returning to the service will reinforce the effectiveness of advertising bans. An alternative approach, that involved providers applying a range of sanctions to advertising account holders that post fraudulent advertisements, would be less effective. Allowing advertising account holders to post further paid-for advertisements after being found to have posted a fraudulent advertisement would provide bad actors with multiple opportunities to post fraudulent advertisements before robust action would be taken against their account. Providers who apply advertising bans, and take

[205] ICO. Online safety and data protection. [accessed 1 May 2026].
[206] UK General Data Protection Regulation, Article 22A to D; ICO, 2026 (in draft at time of publication). Automated decision-making, including profiling. [accessed 10 June 2026].
[207] In the context of preventing return to a service after being banned for posting a fraudulent advertisement, in some instances this may also involve 'storage and access technologies' which engage the requirements set out in regulation 6 of the Privacy and Electronic Communications Regulations (PECR). The ICO has also provided guidance on this matter. See the ICO, Guidance on the use of storage and access technologies. [accessed 22 May 2026].

steps to prevent return, will be better able to prevent known bad actors from continuing to post fraudulent advertisements to the service.

5.88 We expect costs for this proposed measure to be modest as most services already operate the core systems needed to implement account-level bans as part of their wider fraud safety or compliance frameworks.

5.89 We recognise that the proposed measure will present an interference with rights to freedom of expression and privacy. However, we consider any impacts on freedom of expression rights and privacy rights that come from this measure are proportionate to the Act's legitimate objective of protecting individuals in the UK from fraudulent advertising, and note that any interference is subject to safeguards we have introduced through the relevant proposed appeals measures.[208]

5.90 Our provisional view is therefore that it is proportionate to recommend that Category 1 and Category 2A service providers ensure that advertising account holders that post fraudulent advertisements are banned from posting further paid-for advertisements, and that providers take reasonable steps to prevent banned advertising account holders from returning to the service.

5.91 The full text of the measure can be found in the draft Fraudulent Advertising Code of Practice for user-to-user services and in the draft Fraudulent Advertising Code of Practice for search services, and they are referred to as FAU H5 and FAS H5 respectively.

[208] FAU D1, D2, D4, D5, J1, J2, and J4; and FAS D1, D2, D4, D5, J1, J2, and J4.

6. Account appeals

What is this section about?

Account appeals systems and processes provide a means for advertising account holders to challenge decisions taken by Category 1 and 2A providers about the account or an account-level restriction. These proposed measures are intended to ensure that advertising account holders can seek a review of decisions affecting their account and provide relevant information where they believe action has been taken in error or without sufficient context.

In this section, we set out our proposed measures for account appeals and why we are proposing to recommend them.

Our proposals

Number in our Codes	Proposed measure applicable to providers of Category 1 and 2A services
FAU J1 and FAS J1	Providers should have **account appeals systems and processes** which enable advertising account holders to make **account appeals** in a way which will secure that the provider will take appropriate action in relation to them.
FAU J2 and FAS J2	The **systems and processes** should be operated to ensure that the processes for making account appeals **are easy to find, easy to access and easy to use** while considering the likely accessibility needs of advertising account holders.
FAU J3 and FAS J3	The provider should **determine account appeals** promptly.
FAU J4 and FAS J4	Where the provider upholds an **account appeal**, the provider should, as far as possible reverse the action taken as a result of that decision with the purpose of **restoring the complainant or the position of the relevant paid-for advertisement** (or both) to what it would have been had the decision not been made.

Why are we proposing this?

Effective account appeals systems and processes are essential to enable advertising account holders to promptly inform providers of potential errors in decision making. This will ensure decisions can be reviewed, and where appropriate, reversed in a timely and proportionate manner. We set out the detailed rationale for why we consider our proposed measures are an effective approach to enabling account appeals and addressing disputes arising from account-level restrictions and other account integrity Code measures.

Consultation question

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

Introduction

6.1 We propose that Category 1 and Category 2A service providers (providers) should implement account appeals systems and processes for all advertising account holders that have had action taken on their account.[209]

6.2 Account action can be taken on advertising account holders in response to the determination of fraudulent advertisements or failed account checks. While such actions are an important tool for maintaining service integrity and mitigating harm, there may also be circumstances where account actions can affect advertising account holders in instances of error. Robust appeals systems and processes are therefore necessary to ensure that actions taken on an account are fair, proportionate and subject to appropriate oversight.

6.3 We consider that the absence of effective account-level appeals systems and processes could result in some advertising account holders being incorrectly prevented from using the advertising functionality of their account.

6.4 The proposed measures in this section address appeals to account-level actions that have been taken as a result of our proposed account integrity Code measures. This includes action taken as a result of measures proposed in Volume 3 Sections 2 to 5. Volume 4, Section 4, 'Advertising complaints' addresses appeals relating to action that has been taken by the provider against paid-for advertisements, such as banning as a result of determining the paid-for advertisement is fraudulent.

6.5 We acknowledge that a Category 1 or Category 2A service may be serving paid-for advertisements to its users through different advertising pathways. Where relevant, the advertising intermediaries measure would apply. It states the provider should use all reasonable endeavours to implement a version of any measures it has been unable to apply. For more information, see Volume 2, Section 2, 'Advertising intermediaries'.

Account-level appeals

Explanation of these measures

6.6 Advertising account holders may lose complete access to advertising functionality or have a restriction placed on them following checks and actions carried out under the proposed Volume 3, Section 2, 'Account checks and actions', Volume 3, Section 3, 'Preventing fraudulent financial services advertising', and Volume 3, Section 5 'Advertising bans' measures. We propose to recommend that service providers implement systems and processes that allow advertising account holders to appeal decisions taken by providers and to submit additional information when this happens.

6.7 In the draft Fraudulent Advertising Codes, there are a number of types of appeal that advertising account holders can make. This section sets out our proposals that providers should allow advertising account holders to submit appeals for the following reasons:

- failing an account check under Volume 3, Section 2, 'Account checks and actions';

[209] See Annex 7, 'Glossary' for our definition of 'advertising account holder' and Volume 1, Section 3, 'Online advertising ecosystem' for more information about the different types of persons who may use an advertising account. For the purpose of these measures, this also applies to prospective advertising account holders attempting to set up an advertising account.

- failing financial services verification or other actions taken in relation to a breach of the provider's financial services policy under Volume 3, Section 3, 'Preventing fraudulent financial services advertising';
- a restriction being placed on their account under Volume 3, Section 2, 'Account checks and actions'; and
- which advertising account holder has been banned, under Volume 3, Section 5, 'Advertising bans', on the basis that the ban has been applied to the incorrect advertising account holder.

6.8 These proposed measures do not apply to the types of appeal set out in the following list. Our proposals for how these types of appeal should be dealt with are set out in the relevant sections of this document:

- disputing situations involving suspected account takeover under Volume 3 Section 4, 'Countering account takeover'; and
- disputing where an advertisement has been incorrectly referred to as fraudulent under Volume 4, Section 4, 'Advertising complaints'.

6.9 The appeals systems and processes can be the same for both advertising appeals as in Volume 4, Section 4, 'Advertising complaints' and account-level appeals depending on how the service provider has set up their reporting, provided they are handled in accordance with the recommendations of these proposed measures.

6.10 We set out in the following list the expectations about the appeals systems and processes providers should have for account appeals. These are:

- Appeals systems and processes should be easy to find, access and use; including:
  - be easy to find and easily accessible;
  - be designed so they only include reasonably necessary steps;
  - allow advertising account holders to provide supporting information; and
  - have regard to the likely accessibility needs of UK advertising account holders.
- Appeals should be determined promptly.
- Appropriate action should be taken following the appeal.

Appeals systems and processes should be easy to find and easily accessible

6.11 Following action taken on the account or account-level restrictions on the advertising account holder, a clear and accessible route to appeal should be provided. This will ensure that advertising account holders can challenge account-level decisions taken by the service provider and, where an appeal is upheld, that actions taken can be reversed, as far as is appropriate or possible.

6.12 If advertising account holders struggle to understand or locate a route to appeal, they are less likely to submit an appeal to providers, which could leave advertising account holders incorrectly prevented from using the advertising functionality of their account.

6.13 While there should be flexibility in how this is designed, the appeals systems should be easy to find and use. This may include the provider sending a direct link to initiate an appeal to the advertising account holder once the decision has been made, or easy access to a help or appeal form (for example, in business help pages on the service's website).

Appeals systems and processes should be designed so that they only include reasonably necessary steps

6.14 Providers should ensure that the appeals systems and processes used for account-level appeals include only those steps that are reasonably necessary to process an appeal and determine an outcome. The benefit of only including necessary steps is that advertising account holders can more easily submit appeals without the process for doing so being obstructive, and without having to submit more information than necessary for the appeal to be processed.

6.15 This means that service providers may have different numbers of steps depending on factors such as the appeals mechanism used, the grounds on which the appeal has been logged (see paragraph 6.7 for the different grounds of appeal), the information required to assess the appeal, and how that information fits into internal workflows for handling account-level appeals.

6.16 We consider that a balance is required between making the appeals systems and processes quick and easy to use and ensuring the provider has the necessary information to handle appeals promptly and take appropriate action.

Advertising account holders should have the ability to provide supporting information

6.17 The advertising account holder should be able to submit additional supporting information to supplement their appeal. The appeals systems and processes should be designed to ensure the service provider is able to understand the context of the appeal and take informed action on the account.

6.18 This additional information will be beneficial to the provider, so that it can better understand why the advertising account holder has made the appeal and can perform a more accurate assessment of the appeal.

Accessibility of the appeals systems and processes

6.19 We also propose to recommend that service providers consider the likely accessibility needs of advertising account holders that use the account appeals systems and processes. They should do this by having regard to:

- relevant information they hold on their advertising account holders when designing their appeals under the advertising complaints systems and processes, including the needs of those who are disabled; and
- industry standards and good practice on accessibility for disabled people, including implementing assistive technologies to increase the systems' usability (such as keyboard navigation and screen-reading technology).[210]

Prompt determination

6.20 A service provider should also determine account-level appeals promptly. This is in accordance with our proposed measure relating to appropriate action for determining advertising appeals.

---

[210] Volume 4, Section 2, 'Advertising complaints' sets out that service providers should design their advertising complaints systems and processes to take into account the accessibility needs of its UK userbase, including advertising account holders. Under the proposed account appeals measure, the service provider should take into account the specific needs of its advertising account holders on the service.

6.21 This is particularly important for advertising account holders that have had an incorrect decision taken on their advertising account and who may lack the resources or alternative means to maintain their presence or activity on the service if action is taken on their account. For many, the ability to post paid-for advertisements to UK users is an essential aspect of their business activities. Further disruptions can also have a disproportionate impact where there are undue delays to having restrictions on account functionality reversed following an appeal being upheld.

6.22 In Volume 4, Section 4, 'Advertising complaints' we set out examples of how providers could design their systems and processes to determine the outcome of an appeal 'promptly'.

Appropriate action

6.23 Service providers should take appropriate action following determination of the account appeal. Where an account appeal is upheld, the service provider should reverse the actions taken in line with the grounds of each appeal and proportionate to the action taken on the account, so far as appropriate and possible.

6.24 Where an appeal is upheld, the provider should take the following actions in relation to the following types of appeal:

- Failing an account check: Providers should reverse the action taken following an account check and allow the advertising account holder to advertise paid-for advertisements on the service, in line with the provider's account checks and action policy.
- Failing financial services verification or breaching the financial services policy: Providers should reverse the action taken following financial services verification and allow the advertising account holder to advertise paid-for financial services advertisements on the service, in line with the provider's financial services verification policy. Or, where a relevant paid-for advertisement which is not a fraudulent advertisement has been removed on the basis that it is in breach of the provider's financial services policy, the provider should restore the content where it is not found to be financial services advertising.
- Having a restriction placed on the advertising account: Providers should reverse a restriction placed on an advertising account holder and allow increased or full advertising functionality, in line with the provider's account checks and action policy.
- Disputing which advertising account holder was banned: Providers should assess whether an advertising ban would be more appropriately applied to other advertising account holders in connection with the fraudulent advertising posted. Where this is the case, providers should revoke the original decision to impose the advertising ban on the affected advertising account holder and instead impose the advertising ban on those advertising account holders identified as more appropriate.

Benefits and effectiveness

6.25 The primary benefit of these proposed measures is that it safeguards freedom of expression when advertising account holders are incorrectly prevented from using the advertising functionality of their advertising accounts. Such situations can arise from errors made by service providers during checks processes, or from inadvertent mistakes potentially made by advertising account holders when submitting required information. They can also arise

from decisions on which advertising account holder to ban following a provider's determination that a fraudulent advertisement has been posted.

6.26 Ofcom research found multiple instances where advertising account holders faced difficulties engaging with services. In particular, advertisers reported challenges with advertising account-related processes, including reporting issues and account setup.[211]

6.27 We want to ensure that all advertising account holders who are prevented from posting paid-for advertising due to checks, restrictions or bans applied to their account can receive a prompt determination of their appeal.

Impacts and costs on service providers

Direct costs for service providers

6.28 Service providers can use the same underlying appeals systems and processes for both advertising appeals and account appeals, as long as they are handled in accordance with the recommendations of our respective proposed measures. If providers were to do this, we do not expect these proposed measures on account appeals to involve any material costs to providers, in addition to the costs we have already considered for our proposed measures in Volume 4, Section 4, 'Advertising complaints'.

6.29 These proposed measures could result in some specific additional steps and therefore some one-off costs, mainly in the form of staff time, associated with the following:

a) implementing the necessary configurations to handle account-level appeals and related workflows;
b) testing the updated configurations and workflows to ensure they work as expected;
c) ensuring that account-level appeals are routed to the correct teams (for example, advertising account onboarding teams);
d) training relevant staff so that they can handle account-level appeals, including how to review any supporting information submitted and guidance on how to determine and action these appeals; and
e) implementing the necessary design features to the relevant reporting interface used to submit account-level appeals.

6.30 At a minimum, we estimate it could take around two to eight weeks of additional full-time work from one software engineer and the equivalent time from another professional occupation staff. Based on this, we estimate that providers could incur one-off costs of between £5,400 and £43,000.[212] There would also be additional costs associated with producing the relevant training materials and training staff to handle the account appeals, which our cost estimate does not account for.

6.31 There may also be some annual maintenance costs in relation to the upkeep of the systems and processes used to provide the appeal mechanism. These are largely likely to be captured as part of the maintenance costs considered for our proposed measures in Volume 4, Section 4, 'Advertising complaints'.

6.32 The main additional ongoing costs with these proposed measures are likely to be in relation to the staff time needed to handle individual account-level appeals. This will involve reviewing the appeals and implementing any actions where appropriate (for example,

[211] Ofcom, 2026. Online advertising pathways: qualitative research report.
[212] Based on our labour cost assumptions as set out in Annex 8.

reversing bans). We expect these costs will depend on the expected volume of account-level appeals received, which in turn will vary by service size and the number of advertising accounts on services. We also expect these costs to further depend on the complexity of the account-level appeals, and the length of time needed to review any supporting information submitted as part of the appeal.

6.33 Many Category 1 and 2A services appear to already offer a means to appeal as part of their current account verification processes.[213] Therefore, we expect the overall additional costs associated with our proposed measures would be low for these providers.

Rights assessment

Freedom of expression and freedom of association

6.34 As explained in Volume 1, Section 5, 'Approach to Code', Article 10 of the European Convention on Human Rights (ECHR) upholds the right to freedom of expression, which encompasses the right to hold opinions and to receive and impart information and ideas without unnecessary interference by a public authority. Article 10 is a qualified right, and we must exercise our duties under the Online Safety Act 2023 (the Act) in a way that does not restrict this right unless satisfied that is proportionate to the legitimate aim pursued. We start from the position that the proposed measures are prescribed by law, in pursuit of a legitimate aim and corresponds to a pressing social need.

6.35 We consider that the rights impacts on freedom of expression in relation to the proposed measures are similar to those we have outlined in the 'Advertising complaints which are advertising appeals' sub-section in Volume 4, Section 4, 'Advertising complaints'.

6.36 We have considered whether the proposed account appeals measures have any negative impacts on the rights of users, interested persons or advertisers to freedom of expression. We consider the proposed appeals measures acts as a safeguard to freedom of expression in relation to the measures we have proposed for Volume 3, Section 2, 'Account checks and actions', Section 3 'Preventing fraudulent financial services advertising' and Section 5 'Advertising bans' and is a vital route to challenge decisions made under these proposed measures. We consider that determining account-level appeals and taking action where possible and appropriate to reverse the impact of an incorrect decision is an important safeguard for the right to freedom of expression and therefore negative impacts are likely to be limited.

6.37 We consider that allowing advertising account holders to submit relevant information or supporting material could positively benefit their rights, particularly where they might have had their access to the service restricted.

Data protection and privacy

6.38 As explained in Volume 1, Section 5, 'Approach to Code', Article 8 of the ECHR confers the right to respect for an individual's private and family life. Article 8 is a qualified right, and we must exercise our duties under the Act in a way that does not restrict this right unless satisfied that is proportionate to the legitimate aim pursued. As noted in relation to freedom of expression, we start from the position that these proposed measures are

[213] For example, TikTok, 2025. Account Suspension FAQs. [accessed 30 June 2026]; Google, no date. Google Ads account suspensions overview. [accessed 30 June 2026]; Meta, no date. Request a review for a restricted advertising account. [accessed 30 June 2026].

prescribed by law, in pursuit of a legitimate aim and correspond to a pressing social need. Article 8 underpins the data protection laws with which service providers must comply.

6.39 We recognise the potential interference with individuals' right to privacy as, in order to comply with these proposed measures, providers will most likely need to process data, including personal data, submitted as part of an appeal. We consider that the impact on the right to privacy and data protection impacts in relation to these proposed measures are similar to those outlined in the 'Advertising complaints which are advertising appeals' sub-section in Volume 4, Section 4, 'Advertising complaints'.

6.40 Service providers will be required to comply with data protection law when implementing these proposed measures, including following the principles of fairness, transparency and data minimisation. We do not expect providers to gather or process more information than is necessary for the implementation of these proposed measures. Providers should also consider appropriate Information Commissioner's Office (ICO) guidance when implementing these proposed measures. The ICO has a range of data protection compliance guidance which we encourage providers to consult.[214]

6.41 We are satisfied that these proposed measures can be implemented in accordance with data protection law. We consider that the safeguards under data protection law, as set out in paragraph 1.40, and in the various pieces of ICO guidance relevant to these proposed measures, will help ensure that the impact on data protection rights is minimised.

6.42 To the extent that the proposed measures involves interference with individuals' rights to privacy, we consider the interference to be proportionate to the Act's legitimate objective of protecting UK users from fraudulent advertising (which these proposed measures are intended to help providers of Category 1 and 2A services to secure).

Provisional conclusion

6.43 All Category 1 and 2A service providers must have in place proportionate systems and processes designed to protect users from fraudulent advertising in accordance with their duties under sections 38(1) and 39(1) of the Act. Our proposed approach is to recommend service providers should implement account appeals systems and processes.

6.44 We consider these proposed measures will offer material benefits. These primarily arise from these proposed measures acting as a safeguard for freedom of expression and minimising the period during which advertising account holders may be unduly restricted from posting paid-for advertising.

6.45 Prompt determination of appeals minimises the length of time during which an advertising account holder may be incorrectly restricted. This is particularly important for smaller advertisers or individual advertising account holders who may be disproportionately affected by erroneous restrictions and lack alternative avenues for redress.

6.46 We also consider the costs associated with these proposed measures to be limited, though they may vary across service providers depending on the volume of appeals they receive.

6.47 Our provisional view is therefore that it is proportionate to recommend that Category 1 and Category 2A services implement account appeals systems and processes.

[214] See UK GDPR guidance and resources | ICO

6.48 The full text of the proposed measures can be found in the draft Fraudulent Advertising Code of Practice for user-to-user services and in the draft Fraudulent Advertising Code of Practice for search services, and they are referred to as FAU J1 to FAU J4 and FAS J1 to FAS J4 respectively.