Innovate Finance response to Ofcom's Fraudulent Advertising Codes of Practice Consultation

12 October 2026

About Innovate Finance

Innovate Finance is the independent industry body that represents FinTech in the UK. Our membership spans challenger banks, payments firms, electronic money institutions, consumer credit providers, credit information providers, alternative credit rating agencies, wallet providers, personal finance applications, RegTech firms and digital asset firms. We represent start-ups, scale-ups and high-growth companies across the UK FinTech ecosystem.

Our ambition is to make the UK the safest place in the world for consumers and businesses to use digital finance. This requires a technology and AI-based anti-fraud strategy which has real-time data sharing at its core and brings together financial services, technology platforms, telecommunications providers, regulators and law enforcement.

Summary

Innovate Finance welcomes Ofcom's proposed Fraudulent Advertising Codes. Fraudulent advertising is a major source of financial and emotional harm, damages confidence in legitimate digital services and imposes substantial costs on consumers, businesses and payment providers.

The case for strong and promptly implemented Codes is compelling. In 2025, 66% of authorised payment fraud originated on online platforms and a further 17% started through telecommunications networks. UK consumers lost £345 million to fraud initiated through those channels.[1] Further analysis of purchase fraud reports between March 2025 and March 2026 found that 68% originated on Meta platforms (source: Lloyd's Bank).[2]

The financial services sector has strong regulatory and economic incentives to prevent fraud. Banks and payment firms reimbursed 89% of authorised payment fraud losses in 2025, but total authorised payment fraud still increased by 19% to £576.4 million.[3] This demonstrates why reimbursement after the event is not enough. The overriding objective must be to tackle this

[1] https://www.ukfinance.org.uk/news-and-insight/press-release/fraud-report-2026-press-release

[2] https://www.lloydsbankinggroup.com/media/press-releases/2026/lloyds/lloyds-to-launch-scam-check-to-help-customers-dodge-online-shop.html

[3] https://www.ukfinance.org.uk/news-and-insight/press-release/fraud-report-2026-press-release

up-stream; preventing fraudulent content from reaching consumers and stopping fraud before money moves.

We therefore support the layered, safety-by-design approach proposed by Ofcom, however it is crucial this is delivered at-pace. In particular, the final Codes should retain robust advertiser due diligence, business and financial services verification, account security, controls to stop banned fraudsters returning, proactive advertisement review, URL matching and deepfake detection.

The measures should be outcomes-focused, technology-neutral and sufficiently flexible to adapt to an adversarial threat. However, flexibility must not become an excuse for weak implementation. Providers should be required to measure and report outcomes, share timely intelligence with other organisations in the fraud chain and demonstrate that their controls are reducing attempted and successful fraud.

We are pleased to see the following measures included in the draft code:

1. Advertiser Due Diligence: We strongly advocate for robust measures encompassing identity verification, Know Your Customer (KYC) protocols, business verification, financial services verification, and mechanisms to prevent impersonation.
2. Platform Integrity and Account Security: Platforms must secure legitimate accounts from takeover, ensure the swift removal of scammers, and prevent them from returning, ensuring that bad actors cannot simply adapt and re-emerge.
3. Advertisement Content Review: Rigorous measures - including proactive detection technology, URL matching, and deepfake detection must be fully embedded into the consultation framework to review ad content effectively.

These proposals **must be kept in the final version** and the **outcomes measured** in order for them to have any meaningful impact. **These Codes are implemented and effectively enforced as soon as possible**; we cannot wait another year for Ofcom to take action.

Key points:

- Fraudulent advertising causes severe financial and emotional harm, undermines legitimate businesses and weakens trust in digital services. The evidence available to Innovate Finance shows that online platforms and telecommunications services are central to the origination of authorised payment fraud, while banks and payment firms continue to bear most of the cost of reimbursement.

- Ofcom's proposed Codes provide an important opportunity to move the system towards prevention, however progress and the timescales for implementation are too slow. Members are strongly of the view this work must be accelerated if we are to protect as many consumers as possible with this work. We support the layered approach and

strongly support retaining robust advertiser due diligence, identity and business verification, financial services verification, account security, controls to prevent banned fraudsters returning, proactive advertisement review and accessible complaints and appeals.

- The final regime should be outcomes-focused, technology-neutral and capable of adapting to new threats. It should require meaningful measurement and effective enforcement, and it should connect with wider real-time data-sharing arrangements across platforms, telecommunications, financial services, regulators and law enforcement.

- Fraud is a networked crime and requires a networked response. Data sharing is key to preventing this and every effort should be made to facilitate and incentivise the proactive sharing of signals and intelligence before a consumer or business encounters a fraud.

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

We broadly agree with Ofcom's assessment. Fraudulent advertising is an adversarial, technology-enabled form of organised crime. Criminals exploit the scale, targeting capabilities and apparent legitimacy of online advertising to reach consumers efficiently. They combine fraudulent advertisements with impersonation, cloned websites, compromised accounts, synthetic identities, private messaging and telecommunications channels. Funds can then be moved rapidly through mule accounts and across borders.

It is particularly important that Ofcom recognises the wider consequences beyond the immediate financial loss. Victims can suffer severe emotional distress, loss of confidence, debt and lasting damage to their financial resilience. Fraud can also make consumers less willing to use digital payments and other innovative financial services – leading to financial and digital exlusion. Consumer trust and safety are essential if innovation and competition are to flourish.

The impact is often particularly severe for those least able to absorb a loss; 17% of payment fraud victims between 2020 and 2023 had annual incomes below £20,000 and lost an average of £3,512 per incident.[4] Of those victims, 71% said the fraud had a major or moderate effect on their economic circumstances.[5]

There is also a significant competitive impact on legitimate firms. Fraudulent advertisements divert customers, misuse brands and create distrust in lawful advertising. Victims of fraud would

[4] https://www.rusi.org/explore-our-research/projects/fraud-and-financial-inclusion-uk
[5] https://www.smf.co.uk/wp-content/uploads/2023/09/The-view-from-the-ground-September-2023.pdf

understandably be less likely to trust brands or outlets they've not heard of, impacting smaller businesses trying to compete in a digital marketplace.

The financial incentives across the fraud chain are not currently aligned. Financial services firms bear direct losses, reimbursement costs, regulatory obligations and reputational harm, while organisations earlier in the chain may still earn revenue from the advertisement or interaction that enabled the fraud. Ofcom's Codes are an important opportunity to place stronger preventative obligations on the services with the earliest and clearest opportunity to intervene.

2. Do you think Ofcom has missed anything important in its analysis?

Ofcom should give greater weight to the fragmentation of intelligence across the fraud ecosystem. Fraudsters operate across social media, search, online marketplaces, messaging services, telecommunications networks, financial services and payment accounts. No single participant sees the whole event. A platform may see the advertisement, advertiser identity and account behaviour. A telecommunications provider may see relevant subscriber or network indicators. A bank or payment provider may see the resulting transaction. Unless these signals are combined quickly, each organisation acts on only a partial picture.

The current response remains too reactive. It is better at examining what happened after money moved than using intelligence across the ecosystem to stop the fraud beforehand. The Codes should therefore be aligned with the development of the Online Crime Centre and wider work on real-time, reciprocal fraud data sharing.

Ofcom should also give greater consideration to the following:

- The movement of victims from a paid-for advertisement into private messaging, telephone calls or cloned websites. The advertisement may be only the first stage of a longer and more complex fraud journey.
- The use of stolen and synthetic identities to create advertising accounts or impersonate legitimate businesses and individuals.
- Agentic and automated services. These could create new risks where software is able not only to recommend an action but to create and place advertisements or execute another action on a user's behalf.
- The interaction between fraudulent paid-for advertising and user-generated fraudulent content, including listings on peer-to-peer marketplaces. We recognise the statutory limits of this consultation, but consumers do not experience these channels as separate regulatory categories.
- The need for measurable outcomes. Providers should report the number of suspected fraudulent advertisements detected, the time taken to remove them, repeat attempts by connected accounts, the reach achieved before removal and the volume of confirmed fraud originating from their service.

- The importance of financial literacy alongside media literacy. A consumer's ability to recognise implausible returns, misleading risk claims or an investment proposition which appears too good to be true can affect susceptibility to fraudulent financial promotions.
- The resources available to law enforcement. Fraud has accounted for more than 40% of crime while receiving less than 1% of police resources.[6] Prevention by platforms is therefore particularly important, but information collected by platforms must also be capable of supporting investigation, disruption and asset recovery.

3. Do you agree with the examples of risky characteristics Ofcom has provided?

We agree with the examples, including impersonation of public figures and trusted brands, cloaked landing pages, unusual URLs, generative AI and deepfakes, and suspicious advertising-account behaviour.

These characteristics should not generally be treated as determinative in isolation. A combination of content, account, device, payment, destination and behavioural signals is likely to provide a more reliable assessment and reduce false positives.

Relevant indicators should include:

- A newly created advertiser account immediately purchasing a high volume of advertisements.
- Sudden and material changes in the subject, target audience, geography or expenditure of an established account.
- Changes to account administrators, payment methods, devices, recovery credentials or linked domains shortly before a campaign begins.
- Advertisements impersonating a regulated firm, senior executive, public figure or government body.
- Claims of guaranteed or unusually high investment returns, artificial urgency or pressure to move into a private messaging channel.
- Landing pages which differ according to the reviewer, device, geography or referral source.
- Redirect chains, shortened links, recently registered domains, unusual domains or domains which closely imitate a legitimate brand.
- Multiple accounts sharing payment instruments, devices, administrators, infrastructure, destination URLs or creative assets.
- Rapid reuse of advertisements, identities or infrastructure associated with a previously banned account.
- AI-generated voice, image or video content which impersonates a real person or creates false endorsements.

[6] https://publications.parliament.uk/pa/cm5803/cmselect/cmpubacc/40/report.html

- Material discrepancies between the identity of the account holder, the business being advertised, the beneficiary of the transaction and the owner of the destination domain.

Providers should continually validate indicators against confirmed outcomes. Static lists will quickly become obsolete and, if disclosed in excessive detail, can help criminals reverse-engineer controls.

4. Do you agree with Ofcom's proposed approach?

We support Ofcom's layered approach, the emphasis on safety by design and the aim of balancing clear requirements with sufficient flexibility to respond to changing criminal methods.Flexibility must not mean light-touch however.

No single intervention will solve fraudulent advertising. Effective prevention requires mutually reinforcing controls across advertiser onboarding, account integrity, content and destination analysis, reporting, moderation, enforcement and appeals. We particularly welcome the emphasis on account-level intervention because preventing a criminal from accessing advertising systems is preferable to removing individual advertisements after consumers have seen them.

The approach should remain technology-neutral and outcomes-focused. Ofcom should specify the protection and level of assurance expected rather than mandate a narrow tool or solution. Basic keyword detection alone is not adequate; criminals alter language and imagery quickly, while common financial terms can generate false positives. Providers should combine automated analysis, account and network intelligence, URL matching, deepfake detection and appropriately trained human review.

The final Codes should retain the measures on advertiser due diligence, identity and business verification, financial services verification, account security, prevention of repeat access, advertisement content review and accessible reporting. These measures must be **implemented and effectively enforced quickly**. Outcomes should then be measured and the Codes updated as threats and technology develop.

The Codes should also fit into a whole-ecosystem response. Ofcom should work closely with the Financial Conduct Authority (FCA), Payment Services Regulator (PSR), Pay.UK, Information Commissioner's Office (ICO), law enforcement and the Online Crime Centre (OCC) so that reporting, intelligence and enforcement are connected rather than becoming another set of siloed processes. Indeed, many of the organisation above compile data on fraud and its attribution and so they are an important part of delivering this policy goal.

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

We consider the burden proportionate to the scale and severity of the harm, particularly for the large Category 1 and 2A providers within scope.

As referenced in our summary, in 2025, 66% of authorised payment fraud originated on online platforms and a further 17% through telecommunications networks. UK consumers lost £345 million to fraud initiated through those channels. Authorised payment fraud increased by 19% to £576.4 million, even though banks and payment firms reimbursed 89% of losses.[7] These figures demonstrate that significant action is required at source.

Many of the largest providers possess substantial financial resources, sophisticated data capabilities and detailed information about advertisers, account behaviour and advertisement distribution. It is reasonable to expect controls which are commensurate with those capabilities and the risks created by the service.

Proportionality should nevertheless be assessed by reference to risk, size, reach, the provider's degree of control and the design of the advertising pathway. Requirements should not become a rigid checklist that discourages providers from using better technology or concentrates compliance in the largest incumbents. The test should be whether consumers receive an appropriate level of protection and whether the provider can evidence the effectiveness of its approach.

The costs of prevention should also be considered against the costs currently imposed on other parts of the ecosystem. Banks and payment firms face reimbursement, operational and regulatory costs after fraud has occurred. It is fair and proportionate that platforms which control advertising access, targeting and distribution bear meaningful costs to prevent the harm at source.

6. Do you agree with the proposal on advertising intermediaries?

We agree that the use of an advertising intermediary should not result in a lower level of protection for consumers. Providers should not be able to avoid responsibility by choosing a more complex advertising pathway or outsourcing functions to third parties.

The proposed duty to use all reasonable endeavours is a sensible alternative where a provider genuinely lacks sufficient control to implement a measure directly. However, the final Code should make clear that commercial or contractual inconvenience does not in itself amount to insufficient control. A provider should be expected to use its procurement, contracting, technical integration, monitoring and enforcement powers to secure an outcome as close as possible to the relevant measure.

[7] https://www.ukfinance.org.uk/news-and-insight/press-release/fraud-report-2026-press-release

Providers should document:

- Which party controls each stage of the advertising pathway.
- Why the provider cannot implement the measure directly.
- The contractual and technical steps taken to require the intermediary to act.
- The information exchanged between the provider and intermediary.
- The assurance obtained that the intermediary's control is effective.
- The remedial action available if the intermediary fails to meet the required standard.

The provider displaying the advertisement retains an important relationship with the user and should remain accountable for assessing whether the overall control environment protects UK users effectively.

7. Comments on Ofcom's illustrative examples and additional examples of reasonable endeavours

Additional examples of how providers could work with or require intermediaries to implement safety measures include:

- Contractual requirements for intermediaries to carry out advertiser identity, business and financial services verification to an agreed minimum standard before advertisements are placed.
- A requirement for intermediaries to retain and provide auditable verification records, while complying with data-protection and data-minimisation requirements.
- Real-time APIs for sharing advertiser identifiers, destination URLs, account changes, fraud indicators, moderation decisions and confirmed fraud outcomes.
- Contractual service levels for suspending suspected advertisements and accounts, including faster action for high-risk financial services advertisements or impersonation.
- A requirement for intermediaries to block the reuse of payment instruments, devices, domains, administrators or other identifiers connected with banned accounts, subject to appropriate safeguards.
- Joint testing of controls, including sample-based assurance, red-team exercises and mystery-shopping activity.
- Rights for the provider to audit the intermediary's controls and require remediation where performance falls below agreed standards.
- Requirements for intermediaries to preserve relevant evidence for law-enforcement enquiries and account appeals.
- Escalation procedures allowing banks, payment firms, regulators and other trusted flaggers to report suspected fraudulent advertisements directly.
- Suspension or termination rights where an intermediary repeatedly fails to meet the required safety standard.

Ofcom should expect providers to use the leverage reasonably available to them, including contractual renewal and purchasing decisions. The strongest incentives will arise when safety performance affects whether an intermediary is permitted to continue supplying advertising to the service.

8. Do you agree with the proposal on fraud indicator assessments?

We agree. Fraudulent advertising is an adaptive threat and providers need a structured process for understanding how it manifests on their service. A fraud indicator assessment should improve the targeting and proportionality of account checks, moderation and restrictions.

The requirement to review the assessment annually is an appropriate minimum, but annual review alone is not sufficient. Providers should update their assessment promptly when there is a significant change to the service, advertising technology or threat environment, or when evidence identifies a new fraud typology. Failure to do this leaves consumers open to fraud until the next review is initiated, which could be some time.

The assessment should consider indicators in combination rather than rely on a single characteristic. It should examine advertisement content, advertiser identity, account history, payment methods, devices, administrators, destination domains, redirects, audience targeting and links to previously confirmed fraud.

It should also consider the full lifecycle of the activity. A fraudulent advertisement may lead to a cloned website, private messaging channel, telephone conversation or payment account. The original advertisement can appear relatively benign when reviewed without that wider context.

Providers should also test whether their indicators work in practice. Relevant measures include false-positive and false-negative rates, the reach of fraudulent advertisements before detection, the speed of intervention, recurrence through linked accounts and confirmed fraud outcomes. Governance should protect sensitive detection logic so that detailed indicators are not exposed to criminals which would undermine efforts to prevent fraud evolving.

9. Are there other information sources providers should consider?

Providers should consider a broad range of internal and external information, including:

- Complaints and reports from users, non-users and people who have been blocked by the advertiser.
- Reports from banks, payment providers and electronic money institutions which see the resulting payments and confirmed fraud claims.
- Intelligence from the PSR, Pay.UK, FCA, Cifas, law enforcement, the OCC and relevant government bodies.

- Reports from consumer organisations and other specialist trusted flaggers.
- Chargeback, reimbursement and transaction-dispute data linked to advertisers, destination sites or payment beneficiaries.
- Data on account creation, login behaviour, administrator changes, devices, recovery methods, linked accounts and payment instruments.
- Destination URL and domain intelligence, including registration age, redirect chains, ownership changes, hosting patterns and whether the page shown to a reviewer differs from the page shown to a consumer.
- Signals from telecommunications providers where an advertisement directs consumers to a telephone number or messaging service.
- Previous enforcement action, rejected advertisements, banned accounts and attempts to reuse connected infrastructure.
- Public registers, including Companies House and the FCA Register, where relevant to the identity and permissions claimed by an advertiser.
- Ad-library analysis, including reuse of creative assets and campaigns across multiple accounts or services.
- Threat intelligence from other platforms and advertising intermediaries.
- Anonymised financial crime case data and intelligence derived from Suspicious Activity Reports where lawful and appropriate.

Information sharing should be reciprocal. Platforms should share suspected content and account indicators with banks and payment firms. Banks and payment firms should report confirmed fraud outcomes so the originating advertisement, account, domain or network can be blocked. Common standards and secure APIs will be needed if this is to operate at the speed and scale of modern fraud.

Members report that more niche social media and messaging platforms are now featuring more prominently in their fraud attribution figures in new areas such as investment fraud – it is crucial that they are also part of the information sharing initiatives and are taking action under the codes, even if they are smaller in size than some of their competitors.

10. Do you agree with the proposal on testing advertisement generation tools?

We agree that providers should test advertisement generation tools to identify whether and how they could be used to create fraudulent advertisements or proxies.

The obligation should cover the complete tool and deployment process, not only the underlying model. Testing should examine prompts, uploaded images and audio, templates, automated targeting, destination links, safeguards, account permissions and the ability to generate multiple variants at scale.

Testing should include credible adversarial and red-team scenarios involving:

- Impersonation of public figures, regulated firms and government bodies.
- Deepfake video, voice and images.
- False endorsements and fabricated testimonials.
- Cloned brands, websites and customer-service communications.
- Guaranteed investment returns and misleading risk claims.
- Attempts to evade controls through spelling changes, images, coded language or benign-looking proxy content.
- Generation in languages other than English.
- Automated creation and rapid placement of multiple advertisement variants.
- Agentic tools which can create, place, target or modify campaigns with limited human involvement.

Testing should occur before launch, following significant changes and on an ongoing basis. Providers should use emerging threat intelligence and confirmed fraud cases to update scenarios. They should record identified vulnerabilities, remedial action and residual risk.

The requirement should remain technology-neutral and avoid forcing providers to disclose detailed detection logic publicly. Excessively detailed disclosure could help criminals reverse-engineer safeguards, undermining efforts to prevent fraudsters evolving their approach to avoid detection.

11. Do you agree with the proposal on account checks and actions?

We strongly agree. Robust advertiser due diligence and effective account-level action are essential because preventing a fraudster from entering the advertising system is more effective than removing individual advertisements after they have reached consumers.

The final Codes should retain requirements covering identity verification, Know Your Customer checks, business verification, financial services verification and mechanisms to prevent impersonation. Providers should apply the policy consistently and publish a meaningful summary, while avoiding disclosure of detailed controls that could assist circumvention.

Checks should be risk-based but should establish, as a minimum, the identity of the account holder, the existence and status of the relevant business, the authority of the account holder to act for the person or organisation being advertised and, where relevant, legal permission to promote a regulated financial service. Google previously introduced a policy requiring all advertisers offering a financial advertisement to be regulated by the FCA and members saw a significant reduction in fraud originating from their platform, demonstrating the success this approach can have.

Restrictions should be proportionate to the risk and can include enhanced verification, limits on expenditure or reach, delays before publication, human review, restrictions on links or targeting, temporary suspension and permanent bans.

The annual review should be a minimum. Policies and controls should be updated sooner where threat intelligence, incidents or significant product changes indicate that this is necessary.

12. Views on the specific account checks and any additional checks or actions

a) Verifying that account holders work for, or on behalf of, the individual or organisation they advertise

We strongly support this check. A provider should not rely solely on possession of an email address or a self-declaration. Verification should establish the identity of the individual, the existence of the organisation and the individual's authority to act for it.

Checks could include verified corporate-domain credentials, confirmation by an authorised officer, verification against a trusted business register and reusable digital verification. Where an agency acts for a client, both the agency relationship and the client's authority should be established. Additionally, use of Companies House Director Verification could prove useful here, although it should not be used as a panacea given there are still possibly loopholes allowing people to fraudulently identify themselves – such as via an accountant.

Providers should also compare the advertiser's identity with the destination domain, payment beneficiary, branding and claims made in the advertisement. Material discrepancies should trigger enhanced review.

b) Checks and actions to prevent banned account holders returning

We support the proposal. A ban which applies only to a single username or email address will be ineffective against organised fraudsters.

Providers should use proportionate linked-account analysis, including payment instruments, devices, administrators, recovery credentials, business details, domains, destination URLs, creative assets and behavioural patterns. Providers should share confirmed identifiers across their own services and, where lawful and proportionate, with relevant intermediaries and other services.

Controls must include appropriate safeguards because shared devices, agencies and payment arrangements can create innocent links. High-impact decisions should be capable of human review and appeal.

c) Checks for accounts with indicators of a material risk that they will post fraudulent advertising

We support risk-based checks and restrictions. Relevant indicators include sudden changes in spending, geography or subject matter, recently created accounts launching high-volume campaigns, repeated advertisement rejection, discrepancies between the advertiser and destination site, or links to previously confirmed fraud.

Restrictions should escalate according to risk. A provider might require enhanced verification or human review before applying a permanent ban. This will allow strong prevention without imposing unnecessary friction on every legitimate advertiser.

d) Repeat checks following relevant changes

We support repeat verification when there is a relevant change. Changes to administrators, beneficial ownership, contact details, authentication or recovery methods, payment instruments, destination domains, regulated status or the products being advertised may indicate account takeover or a material change in risk.

Repeat checks should also be triggered by a long period of dormancy followed by sudden activity, an unusual change in advertisement expenditure or evidence that the account's credentials may have been compromised.

Additional checks and actions

Providers should consider:

- Device binding and phishing-resistant multi-factor authentication for advertising accounts.
- Enhanced checks before the first campaign, following dormancy and before a material increase in expenditure or reach.
- Verification of destination-domain ownership and monitoring for subsequent changes or cloaking.
- Comparison of account-holder, business, domain and payment-beneficiary information.
- Screening for connections with accounts, devices, domains and payment instruments associated with confirmed fraud.
- Limits on reach, spend or rapid campaign creation for new or higher-risk accounts until trust is established.
- Human review for high-risk financial services, investment or impersonation cases.
- Monitoring of changes made after initial advertisement approval.
- Secure integration with certified digital verification services.
- Preservation of evidence for complaints, appeals and law-enforcement investigations.

13. Do you agree with the proposal on preventing fraudulent financial services advertising?

We strongly agree. Any individual or firm advertising financial services to UK consumers should be legally permitted to do so. Verification should take place before the advertisement can be encountered by UK users.

Google's policy stated that advertisers must demonstrate that they are authorised by the FCA or qualify for an exemption, and that verification applies to all advertisement formats and assets. This is clearer than language which suggests that a provider may request additional evidence only in some circumstances.

Ofcom should establish a minimum standard. Providers should verify the advertiser against the FCA Register, which is also available via an API, or establish the relevant exemption or approval by an authorised firm. They should not rely solely on an advertiser's declaration.

Verification should be repeated where the advertiser's identity, permissions, approving firm, product, destination domain or other relevant details change. Providers should also respond promptly where the FCA updates a warning or an advertiser loses permission.

The policy should cover advertisements which do not explicitly describe themselves as financial services but which direct consumers towards an investment, credit, payment, cryptoasset or other regulated proposition. Providers should also guard against the misuse of an authorised firm's identity or reference number by an unrelated fraudster.

This measure should operate alongside advertiser identity and business verification, URL and destination analysis, proactive moderation and accessible reporting. Checking an FCA permission alone will not prevent cloned-firm fraud or account takeover.

14. Do you agree with the proposals on countering account takeover?

We agree with both proposed measures.

FAU H3 and FAS H3: account security mechanisms

Every advertising account should have an effective security mechanism. The control should be proportionate to the account's risk and capabilities but should not rely on a single authentication factor.

Providers should promote phishing-resistant authentication, including passkeys, secure multi-factor authentication and device binding. They should monitor unusual devices, locations,

administrators, recovery actions and changes in user behaviour. Higher-risk activity should trigger step-up authentication or temporary restrictions.

Security should extend to recovery processes. A strong login mechanism can be undermined by a weak password reset, administrator invitation or account-recovery route. Providers should be required to notify legitimate account holders of material changes and offer a rapid means of revoking unknown access.

FAU H4 and FAS H4: account takeover reporting

We support a reporting mechanism which is easy to find, access and use, including for an advertiser who can no longer log in. A victim of account takeover should not be required to access the compromised account or locate the fraudulent advertisement before reporting it.

Reports should trigger rapid containment, including suspension of new advertising, preservation of evidence and review of recent advertisements, administrator changes, payment methods and linked activity. Providers should communicate clearly with the legitimate account holder and restore access safely once identity and authority have been established.

The reporting mechanism should be accessible and supported by trained staff. High-risk reports should not be routed solely through a slow general complaints process.

15. Do you have evidence about account takeover that could inform Ofcom's assessment, including how frequently it occurs or its impact?

We do not hold any evidence.

16. Do you agree with the proposal on advertising bans?

We agree that an account holder found to have posted fraudulent advertisements or a fraudulent advertising proxy should be banned and that reasonable steps should be taken to prevent their return.

The effectiveness of the measure will depend on whether the ban applies to the underlying actor and connected infrastructure rather than only the individual account. Fraudsters can otherwise return using a new email address, account name or business identity.

Providers should use proportionate analysis of connected accounts, administrators, payment instruments, devices, domains, recovery credentials and advertisement assets. They should also review other live advertisements and accounts which appear to form part of the same network.

The threshold and evidence for a ban should be recorded. Where the evidence is sufficiently strong, providers should act quickly to prevent continuing harm. The existence of an appeal should not automatically require a high-risk account or advertisement to remain active while the appeal is considered.

Providers should measure repeat attempts by banned actors and the effectiveness of controls in stopping them. A high volume of repeat access would indicate that the original ban and associated controls are not operating effectively.

17. Are there additional exceptional circumstances in which it may be proportionate to reverse advertising bans?

Reversing a ban may be considered where:

- An appeal demonstrates that the original finding was materially wrong.
- The account was taken over and the legitimate account holder was not responsible for the fraudulent advertisements. Access would obviously need to be reinstated with enhanced security controls before this would be allowed.
- An employee, contractor or agency acted without the authority of the organisation and the organisation has removed access, secured the account and addressed the relevant control failure.
- The account was incorrectly connected to a banned actor through a shared device, payment service, agency or other identifier.
- New evidence demonstrates that an advertisement was lawful and legitimate.
- A provider applied an account-wide ban where a narrower restriction would have addressed the identified risk proportionately.

Reversal should depend on appropriate remediation. This may include re-verification, removal of compromised administrators, replacement of authentication and recovery credentials, review of destination domains and payment methods, and enhanced monitoring for an appropriate period.

A reversal should not simply restore every previous permission automatically. Providers should consider staged restoration, limits on reach or expenditure and pre-publication review where residual risk remains. Accounts may also qualify for enhanced screening for a period of time to ensure the reversal was a correct decision.

18. Do you agree with the proposals on account appeals?

Effective appeals are necessary because identity matching, linked-account analysis and automated moderation can sometimes produce false positives. An incorrect restriction can

cause substantial harm to a legitimate business, particularly an SME which depends on online advertising for sales.

FAU J1 and FAS J1: appeals systems and processes

Providers should maintain a meaningful route through which an advertiser can challenge an account decision and submit relevant evidence. The appeal should be reviewed by a person or system with access to the reasons for the original decision and the authority to reverse it.

FAU J2 and FAS J2: accessible appeals

The appeal route should be easy to find, access and use, including where the advertiser has lost access to the account. Providers should explain the categories of evidence that may assist, such as proof of identity, business authority, FCA permission or evidence of account takeover.

FAU J3 and FAS J3: prompt determination

We agree that appeals should be determined promptly. Ofcom should consider risk-based service standards. A legitimate SME can suffer immediate loss if its principal advertising channel is disabled, while a suspected fraudster should not be allowed to continue reaching consumers merely because an appeal is pending.

FAU J4 and FAS J4: restoration following a successful appeal

Where an appeal succeeds, the provider should reverse the action as far as possible and restore the account and advertisements to the position they would have occupied had the error not occurred. Providers should also correct linked risk signals and automated systems so that the same error is not immediately repeated, but retain enhanced monitoring to ensure the reinstatement was the correct decision.

The appeals framework should preserve an audit trail of the initial decision, evidence considered, outcome and any changes made to the provider's controls. Providers should analyse successful appeals to identify recurring sources of false positives and improve their systems.

Appeals are an important safeguard, but they should not weaken prevention. Providers should be able to maintain temporary restrictions during an appeal where there is a credible and material risk of consumer harm, provided the appeal is handled urgently and the restriction is no broader than necessary.
Fraudulent advertising causes severe financial and emotional harm, undermines legitimate businesses and weakens trust in digital services. The evidence available to Innovate Finance shows that online platforms and telecommunications services are central to the origination of

authorised payment fraud, while banks and payment firms continue to bear most of the cost of reimbursement.

Ofcom's proposed Codes provide an important opportunity to move the system towards prevention. We support the layered approach and strongly support retaining robust advertiser due diligence, identity and business verification, financial services verification, account security, controls to prevent banned fraudsters returning, proactive advertisement review and accessible complaints and appeals.

The final regime should be outcomes-focused, technology-neutral and capable of adapting to new threats. It should require meaningful measurement and effective enforcement, and it should connect with wider real-time data-sharing arrangements across platforms, telecommunications, financial services, regulators and law enforcement.

Fraud is a networked crime and requires a networked response. Every organisation with the data or ability to prevent harm should have both the capability and the incentive to act before consumers lose money.