Which?
2 Marylebone Road
London NW1 4DF
020 7770 7000
which.co.uk

Online Safety Policy Delivery Team
Ofcom
Riverside House
2A Southwark Bridge Road
London
SE1 9HA

Consultation Response

Which? response to the Ofcom consultation on Call for evidence: Third phase of online safety regulation

Submission date: 20/05/2024

Summary

Which? welcomes this opportunity to respond to Ofcom's call for evidence. It is crucial that online services put in place strong protections to prevent fraudsters from using online advertising to reach consumers.
Our evidence shows that:

- Fraudsters use advertising as a mechanism to reach consumers at scale.
- Fraudsters are flexible and use different types of advertising to attract consumers and evade restrictions on specific advertising areas.

In order for online services to protect consumers from fraudulent advertising they must introduce effective onboarding Know Your Customer checks.

- KYC checks are an established element of fraud prevention in financial services and would be a useful addition to online services.
- Checks should be used to establish that there is valid identity associated with the individual or business seeking to advertise and check that they are not associated with previous fraudulent activity.

There are proactive technologies that are useful in detecting fraudulent advertising:

- URL detection techniques can take advantage of a wide range of public sector and private sector data on suspected fraudulent URLs.
- Machine learning and generative AI can be useful technologies for detecting potentially fraudulent advertising.

Full response

Scale and breadth of Fraudulent Advertising and the harm it causes (Q36)

Fraudsters use online advertising as a mechanism to reach consumers at a substantial scale and large search and social media services provide an audience at volume to target. Ofcom's research shows that Alphabet, which owns Google and Youtube, is the organisation whose sites and apps are most visited by UK adults, followed by Meta (owner of Facebook, WhatsApp and Instagram). Ofcom's research also demonstrates the impact of this reach on consumers, with the public highly concerned about the harm from 'scams, fraud and phishing' and likely to report that they have direct experience of encountering it.

Data from Action Fraud suggested that in 2020/21 35,000 frauds could be linked to digital advertising with an estimated cost of £400m. Which?'s analysis shows that this cost is likely to substantially underestimate the total level of harm from online fraud due to underreporting of fraud and the non-financial harms associated with being a victim of fraud. When a consumer falls victim to a scam through fraudulent advertising, they face a number of different harms in addition to financial hams.

Psychological harm may stem from large amounts of capital lost or embarrassment which may contribute to hesitancy in reporting the incident. Which? qualitative interviews with scam victims found that they reported feeling substantive distress at realising that they had been scammed. In addition, Which? quantitative research found that being a victim of a scam is associated with lower levels of life satisfaction and happiness, and higher levels of anxiety. Using HM Treasuary's guidance on well being analysis this translates to an average impact of £2,509 per scam victim.

Crest Advisory research also found that 20% of victims of fraud said their physical health had suffered, 32% reported a psychological impact, 42% were affected financially, 47% experienced an emotional impact, 23% experienced anxiety, 12% experienced disturbed sleep and 11% experienced depression.

It is critical to note that the Which? research found scam victims of different ages, gender and socio–economic status fell victim to scams in periods of significant distraction, acute stress or serious emotional strain rather than vulnerability to scams being linked to specific demographics. This evidence is vital to help build detection and preventative measures that look across all online consumers and the full suite of advertising, rather than adverts that target specific demographics.

The variety of fraudulent adverts

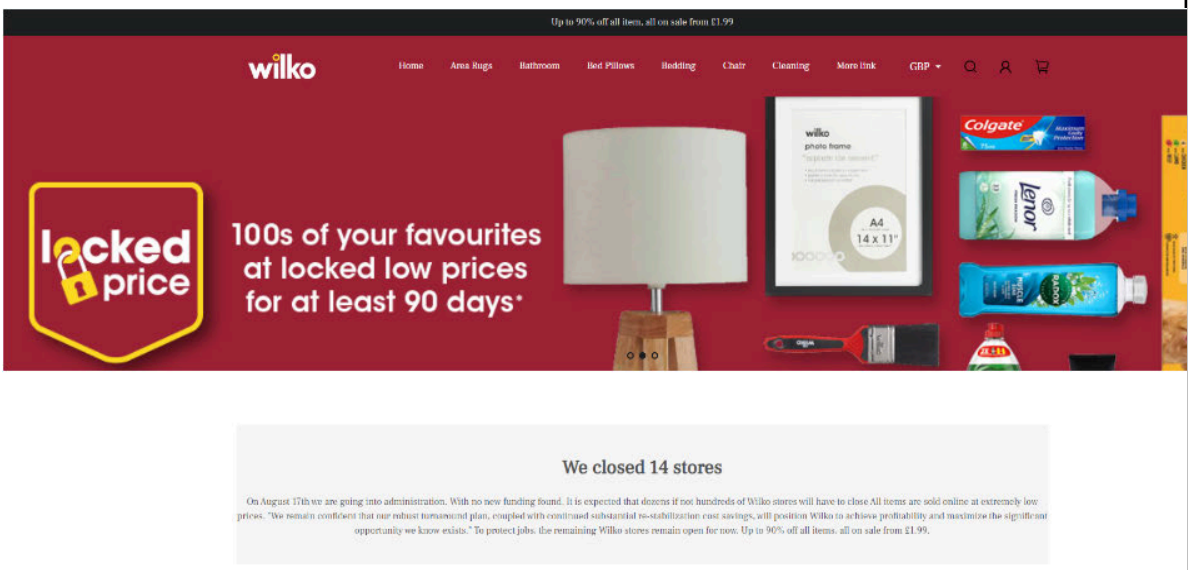
Fraudsters focus on advertising that is effective at connecting with consumers, rather than having a preference for a specific product or service. They take advantage of trends using news stories and celebrities to attract attention. We have accumulated evidence via a wide range of published investigations in addition to our own research that details the wide variety of types of fraudulent adverts which cause consumer harm. These are present on both

search engines and user to user services. Fraudster's adaptability suggests that attempts to reduce harm by focusing on specific types of advertising may be easily circumvented. A clear example of this is how fraudsters evade checks on investment adverts through generic adverts that in fact redirect victims toward an investment scam as seen in example I below.

Advertising Case Studies:

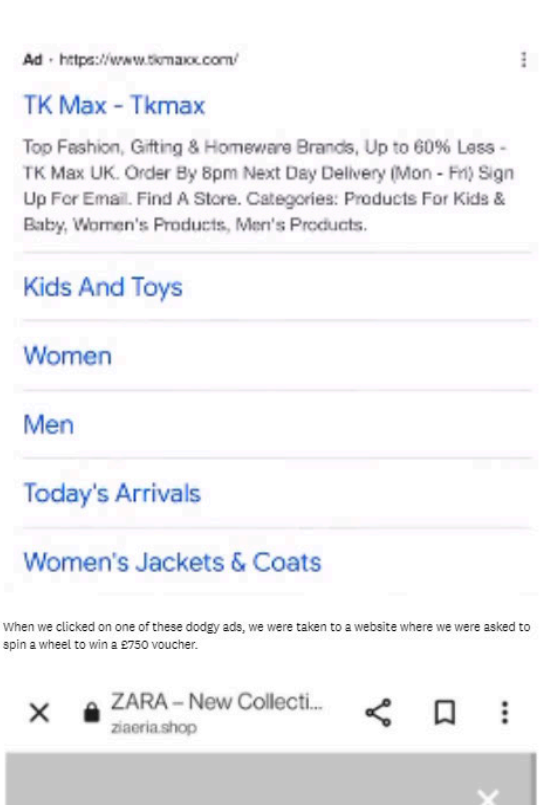
A: <u>Instagram advert impersonating a clothing brand</u>. The consumer purchased discounted items from what was assumed to be retail brand, Paul Smith.

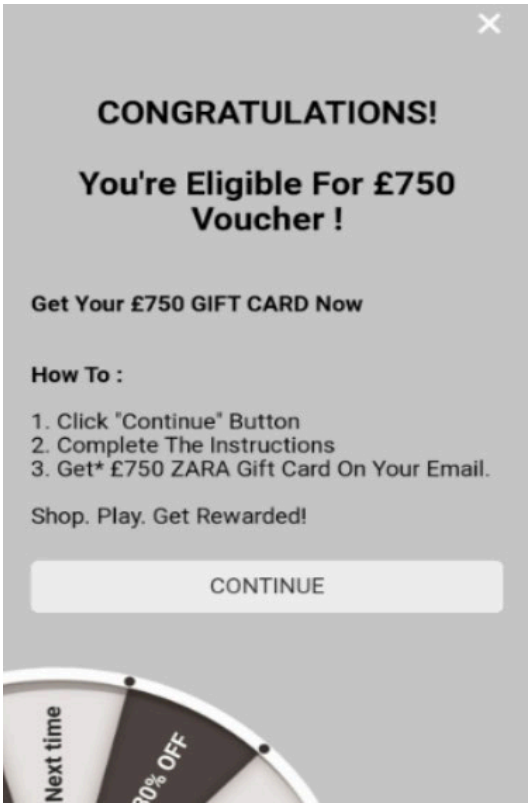
B: <u>Adverts on Facebook impersonating collapsing retail brands.</u> Which? investigations found fraudulent adverts impersonating <u>Wilko</u> and <u>Cath Kidston</u> which advertised closing down sales with sharp discounts to lure in potential victims.



A scam website impersonating Wilko

C: <u>Google adverts on search results for major retailers.</u> Google allowed fraudsters to pay for advertising which would push their advert to the top of search results when shoppers looked up popular retailers on Google. These adverts often state the retailer's URL, but when victims clicked on the advert, they are taken to a different website offering rewards, where victims are promised a shopping voucher in exchange for completing a series of tasks. In reality, victims are handing over their personal data.





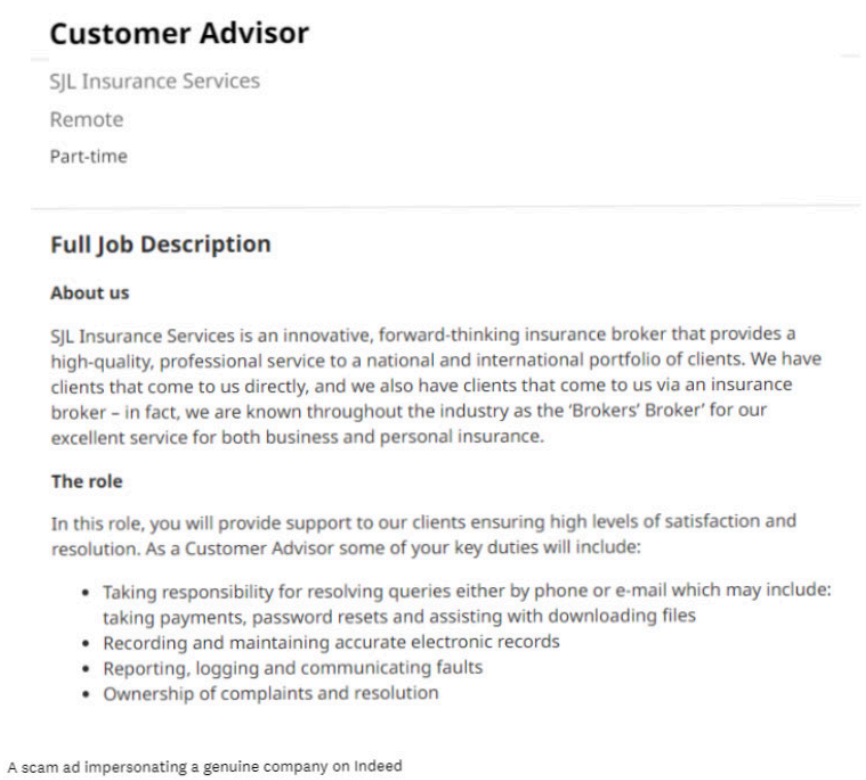
D: <u>Adverts on meta platforms advertising pets for sale</u>. Scammers keep tabs on which breeds are in high demand, taking photos from the internet and sharing fictitious information about the animal to create the appearance of authenticity and following the steps of a reputable seller.

Once money has been sent for the animal, the advert and scammer will disappear.

E: <u>Adverts on Instagram impersonating a car leasing firm</u>. The advert impersonated a legitimate firm, taking information from Companies House to convincingly replicate invoices. A £3,000 deposit was paid and the car was never delivered.

Which? first became aware of the advert in November 2023.The fraudulent Instagram profile briefly went offline (it is unclear whether Instagram or the scammers themselves were responsible), but it wasn't permanently banned from the platform, despite being reported to Meta by both the legitimate business owner and Which?. The profile reappeared under a new name and remains live as of April 2024. The 'About this account' page on the profile reveals it had existed under six different names in the eight months since it was created.

F: <u>Adverts on Indeed for jobs.</u> Which? carried out an investigation into a role advertised on Indeed. The scammer used the name of a genuine employee for the company to hire money mules to transfer funds illegally between accounts via a genuine cryptocurrency platform.



Customer Advisor

SJL Insurance Services

Remote

Part-time

Full Job Description

About us

SJL Insurance Services is an innovative, forward-thinking insurance broker that provides a high-quality, professional service to a national and international portfolio of clients. We have clients that come to us directly, and we also have clients that come to us via an insurance broker – in fact, we are known throughout the industry as the 'Brokers' Broker' for our excellent service for both business and personal insurance.

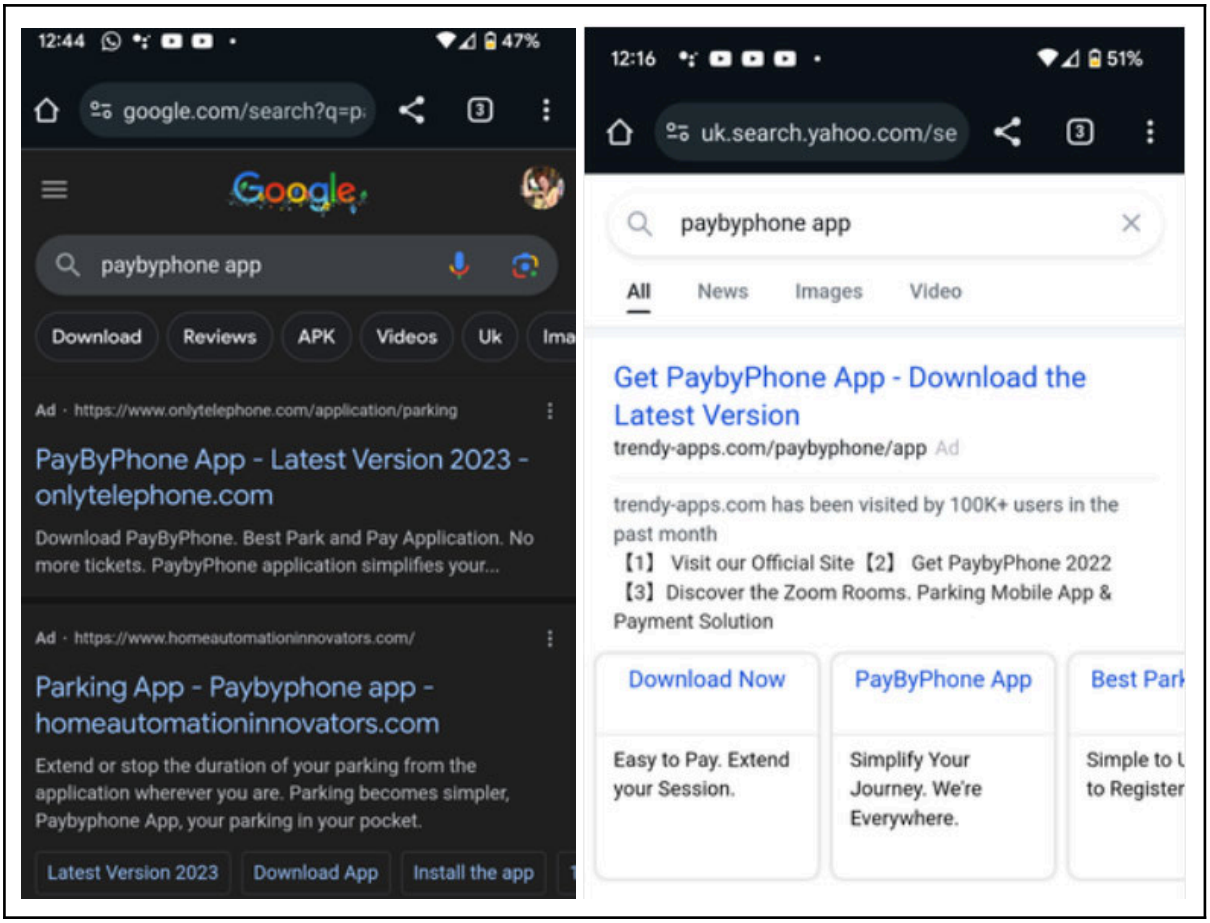
The role

In this role, you will provide support to our clients ensuring high levels of satisfaction and resolution. As a Customer Advisor some of your key duties will include:

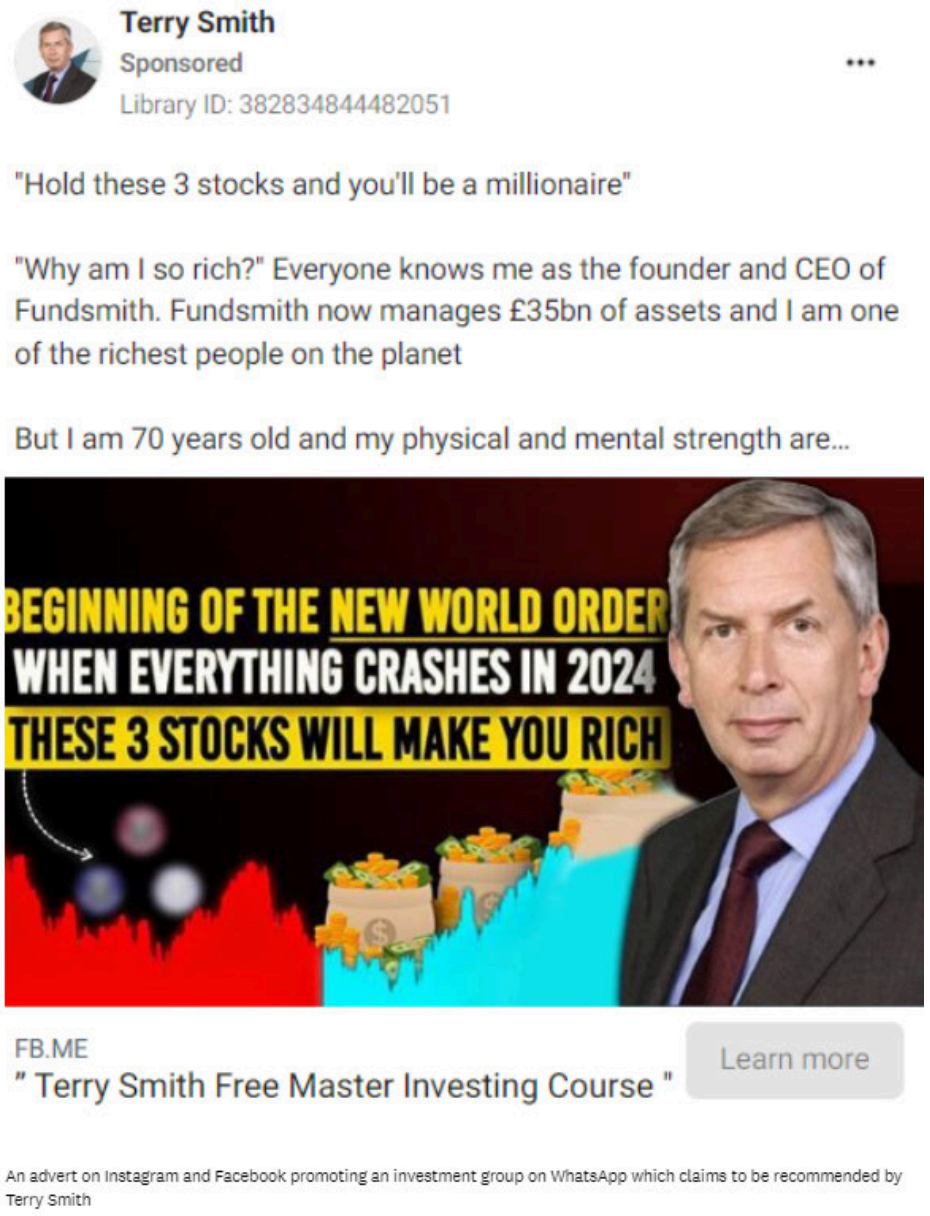
- Taking responsibility for resolving queries either by phone or e-mail which may include: taking payments, password resets and assisting with downloading files
- Recording and maintaining accurate electronic records
- Reporting, logging and communicating faults
- Ownership of complaints and resolution

A scam ad impersonating a genuine company on Indeed

G: <u>Adverts for scam parking services on major search providers</u>. Which? investigations found adverts for scam parking services on Google, Bing and Yahoo. These services advertise parking services impersonating a real parking payment provider and sign customers up to unrelated expensive subscriptions.



H: <u>Adverts on Meta platforms for fraudulent investment training</u>. Which? has recently reported on scam adverts on Facebook and Instagram that claim to be celebrity endorsed investment training courses.



An advert on Instagram and Facebook promoting an investment group on WhatsApp which claims to be recommended by Terry Smith

I: <u>Hidden investment adverts on X</u>. Investigations have found a variety of adverts on X showing celebrities with cryptic text claiming they have access to secret information. These lead to fake articles that direct potential victims to fraudulent investment opportunities.

J: <u>Click-to-dial advert on Bing impersonating an airline</u>. Which? has recently reported on scam adverts that appeared on Bing when individuals searched for British Airways on a mobile device. When the link in the advert is clicked it takes the individual into their phone call function with a preloaded number. That number is unrelated to British Airways and when Which? called it, requested sensitive data.

Verification in advertising (Q44)

Large online services should be required to complete onboarding and verification checks of businesses or individuals registering to publish advertisements before any advert is published and displayed to consumers. This should be proactive and preemptive to prevent fraudsters reaching consumers in the first place and can be completed through Know Your Customer ('KYC') checks. KYC is already an effective preventative procedure in the financial sector and included within Financial Conduct Authority (FCA) regulations. KYC encapsulates both the verification of the business or individual and their eligibility to access the service. We believe a similar application of verification requirements will provide a barrier to bad actors before they are able to do harm to the consumer. We recommend a model where a business or individual is required to provide robust data evidence that they are legitimate to support their request to advertise and reach consumers at scale. When the director of enforcement and market oversight at the FCA discussed the Online Safety Act, he also noted the opportunity and value of KYC "standards around how these sites (fraudulent) get on the internet in the first place" noting them as important to prevent fraud and move away from a game of "whack-a-mole" with fraudsters.

KYC has not solely been reserved for financial service protections and has been used in a variety of sectors to prevent illegal activity. Evidence from the organisation Know Your Business Customer (KYBC), a collection of businesses that provide these services, uses the following examples:

KYC results in a reduction of illegal activities online Since DK Hostmaster in Denmark implemented the verification of business user details through NemID, illegal activities were reduced from 700 instances in 2016 to 8 in 2019.
KYC used to prevent NFOrce hosting child pornography Introducing simple KYC obligations that verify business user details against existing databases within the EU means easily tracing anonymous operators offering illegal products and services.
Lack of KYC checks results in limited traceability of third-party sellers Illicit trade in non-branded toys relied on e-commerce platforms, social media and instant messaging services. Approximately 76% of non-branded toys ordered from 3rd party sellers were unsafe for children. Limited application of KYC led to difficulty tracing sellers, creating a further challenge for law enforcement and dismantling networks. As a result further harm was not prevented by effective enforcement action.

Which? have identified that the current online advertising ecosystem is voluntary in its approach. The two primary bodies are the Interactive Advertising Bureau (IAB) and the Trustworthy Accountability Group (TAG) which advertisers can certify to having implemented certain processes to receive a gold standard, or the certified against fraud seal (CAF). However, this model was primarily designed to prevent fraudsters from abusing the industry rather than protecting consumers and has resulted in poor understanding of bad actor behaviour or consumer harm within the industry collected data.

The IAB's gold standard contains an example of KYC for consumer protection built in. FCA registration for financial advertising is required to legitimise an advert. We note that many large platforms require that any advert promoting financial products or services that target UK audiences need to be authorised with the FCA. The Times previously revealed that since Google's refusal to allow financial adverts on their platform from companies not registered with the FCA, the number of people falling victim to fraudulent websites appeared to reduce with TSB reporting a large reduction. However, Which? believes that use of FCA data alone does not go far enough to tackle the depth and breadth of tactics used by bad actors. We must see advertisers held to wider, rigorous checks on behalf of the consumer.

The Government's Online Fraud Charter requires that signatories with paid advertising services deploy verification measures for new advertisers. Which? has heard from major platforms that they are currently A/B testing verification measures that they hope to have in effect for at least some new advertisers by the end of the 6 month implementation period of the charter.

A framework for KYC

An effective KYC process must verify online advertisers and be able to verify they have a legitimate right to access to the service. Our extensive research into best practice for KYC clearly demonstrates that multiple data sources must be used in this process.

For advertisers on large online services we recommend that the information provided by businesses or individuals is checked against public sector, regulator, trade body and private data. Our engagement with multiple sector stakeholders has shown that there is already a variety of verification processes that are currently being used to detect fraud risk indicators. Examples include real time video technology to authenticate recognised photo ID, looking for abnormal patterns of behaviour or simply to verify a history of genuine activity associated with the identity. Businesses use data sources such as email risk scores and credit reference agencies like Equifax, and Experian.

Services who deploy KYC told us that their processes were designed to have a 'happy path' and a path for exceptions. The happy path is designed for the least friction for the user and cost efficiency for the business. These tend to consist of a high certainty easy-to-use identity check that could be used to establish whether the vast majority of users were genuine (like a video ID check). Those who failed or could not participate in those checks (the exceptions) were funnelled to some of a variety of additional checks depending on what data about them was available. This approach enables proportionality for both the user and the business. This methodology is designed for a full spectrum of users and incorporates multiple data sources. This means that a user without physical ID can still verify via a different data pathway, equally someone without a mobile device to take a video could participate.

KYC can be an ongoing process to prevent malicious use. Google has implemented a 'get-to-know-you' period for advertisers who don't yet have an established track record of good behaviour, during which impressions (reach) for their adverts might be limited. We are aware from discussions with other large platforms they are using or considering a similar approach. We recommend this in our suggested framework as an alternative way, where

there is a lack of history data against a business or individual, of reducing harm whilst establishing genuine activity.

In the long term, to ensure KYC checks are robust and accurate, large online services should be conducting two checks against businesses or individuals who request online advertising space. Firstly, a verification check to effectively confirm that the business or individual is legitimate. This could include using a digital identity scheme or other Government data that establishes an individual as having a genuine identity. Secondly, an online service provider should check for any indicators of fraudulent activity against the business or individual asserted identity. We describe the multiple data sources potentially available below. Which? would like to highlight that new sources of fraud indicators should be made available, including Government owned such as HMRC, to help widen the breadth of prevention data. Figure 1 provides a list of the types of identifiers available and possible data sources these could be checked against.

Figure 1 Framework for KYC

Business and Individual identifiers	**Data sources to check against**
An identifier will be used to check against data sources that will provide both verification of a match and history that shows no fraud indicators.	
Individual Identifiers: ● Recognised Photo ID (Passport, Drivers licence etc) ● Personal Email address ● Personal Address ● Payment Method ● Device ID ● IP Address ● Phone number ● Registration behaviour ● Previous Account activity on the service **Business Identifiers:** ● Business legal name ● Any addresses associated with the business ● The country of its incorporation ● A registered identifier such as; ○ HMRC Tax/ VAT Number ● Data Protection Registration Number ● Companies House Number	**Sources to check:** ● Services' Internal Data* ● Anti Fraud service such as CIFAS + ● Information brokers such as Experian + ● FCA warning list* ● Financial Services Register* ● Register of data protection fee payers* ● Companies House* ● Payment provider such as Mastercard + ● HMRC ● Trading Standards ● Digital identity scheme *currently freely available + currently available for a cost

We also recommend that Ofcom continue to consider the development of a data sharing ecosystem between online services. Fraud indicator data generated on the online services is a rich source of bad actor behaviour and will help feed into these effective

KYC checks. Services will then be able to check if an individual or business has a history of fraudulent activity on other platforms when they seek to register for their service.

KYC checks must apply not only to dedicated advertising but also to 'boosted' or 'sponsored' content from individuals. User generated content which acts like advertising (in that it is promoted to users on the basis of payment), also known as boosted content, is covered by the illegal content codes of practice rather than the fraudulent advertising codes of practice. The illegal content codes of practice should be updated to include KYC measures for boosted content.

Which? would also like to draw Ofcom's attention to the fact fraudulent advertisers will react as KYC checks improve. Which?'s stakeholder engagement has revealed warnings that fraudsters' evolving tactics would likely include using mules to create accounts or compromising existing verified accounts. Ofcom must work with the ICO and NCSC to consider cybersecurity as part of the fraudulent advertising code to prevent account compromise. We note that cybersecurity was not explicitly included in the consultation, but we are hopeful of a recommendation in the upcoming Codes. For example this could include requirements on the level of security required for advertiser accounts such as the use of passkeys.

Consuming data for proactive technology (Q43, Q37)

Fraudsters use URLs in advertising to take potential victims away from an online service to a fraudulent domain that the fraudster controls. URL matching would be an effective tool to detect fraudulent advertising as it is for detecting fraudulent user generated content.

As recommended in Which?'s response to Ofcom's consultation on protecting people from illegal harms, a range of data sources are vital for detecting fraudulent URLs. This applies in advertising as in user generated content. We recommended:

- Internal data e.g. URLs or services previously detected and removed from an online service
- Government provided sources e.g. the National Cyber Security Centre's (NCSC) Share and Defend programme
- Private feeds e.g. those operated by the DNS Research Federation

We are hopeful that Ofcom includes this variety of data sources as recommendations that online services use in the prevention of fraudulent advertising.

We have identified specific sources of data on URLs in fraudulent advertising. The Advertising Standards Authority (ASA) operates the Scam Ad Alert system that shares information about fraudulent adverts with major online service providers. It includes many services providers that are likely to be classified as Category 1 and 2a such as Google, Meta, TikTok, Microsoft, and X. The ASA assesses adverts reported by the public and shares data on the adverts it believes are fraudulent including the URL. In the 12 months leading up to October 2023 the ASA issued 152 Scam Ad Alerts 47% of which related to ads seen on social media sites. Although these are small numbers this is a useful source of free data. Which? consider that if a consumer falls victim to a fraud that has previously been

identified by the ASA, but an online service has not acted on this data, unacceptable. It is shocking that only 50% of ASA alerts are being confirmed as actioned by online services within 48 hours.

There are also industry groups that collaborate to share intelligence about fraudulent advertising in a way that they do not for user generated content. For example the Trustworthy Accountability Group (TAG) operates an intelligence sharing network that shares information about malvertising including fraudulent adverts. This allows different platforms to collaborate and share real-time information about harmful adverts. Companies like The Media Trust offer blocking services using curated block lists that include known scams.

In addition to URL matching, Which?'s illiegal harms response highlighted proactive technology that can be used to detect online fraud. This included Which?'s research using machine learning classifiers and we recommended Ofcom should build its evidence base on the use of techniques like machine learning. We extend this recommendation to tackle fraudulent advertising as well as user generated fraud.

Generative AI (Q49,Q37)

Generative AI is being used to create fraudulent adverts. Which? has noted that AI is used to create fake celebrity endorsements using deep fake technology, providing an element of credibility to the scam. We believe the evolving use of generative AI accelerates the potential rate of harm to consumers. We have noted the following examples:

- Report from the BBC that YouTuber, MrBeast and BBC presenters had been used in deep fake videos to scam unsuspecting people online.
- A scammer paid Facebook $7,000 to reach 100,000 people in Australia with a deep fake video of Australian politicians and well known business professionals seemingly advocating for an investment opportunity which was in fact a scam, as reported by The Guardian.
- Fraudulent deep fake advertisements of Martin Lewis endorsing 'great investment opportunities' linked to Elon Musk.

However, Which? acknowledges generative AI tools do have potential to improve online services detection of fraudulent advertising. In fraudulent advertising, Google is using Generative AI to spot harmful adverts including ones promoting unreliable financial claims, such as get-rich-quick schemes. We recommend that Ofcom consider generative AI from both the bad actor's use and as a preventative tool for online services that could be more accurate, swifter and consistent than existing human or machine learning based moderation. This is being demonstrated by the work of Dave Willner, former head of trust and safety at OpenAI.

About Which?

Which? is the UK's consumer champion, here to make life simpler, fairer and safer for everyone. Our research gets to the heart of consumer issues, our advice is impartial, and our rigorous product tests lead to expert recommendations. We're the independent

consumer voice that works with politicians and lawmakers, investigates, holds businesses to account and makes change happen. As an organisation we're not for profit and all for making consumers more powerful.

For more information contact:

[redacted]

May 2024