sparkninety

Online Advertising Programme Market Insights

Final Report

For the Department of Digital, Culture, Media and Sport

11th July 2022

sparkninety

About Spark Ninety

Spark Ninety is a strategy consultancy focused on the digital media and advertising sectors. It helps clients to understand complex markets and emerging business models; to develop strategies and plans; and to assess investments. Spark Ninety's team are trusted advisors to clients including major technology, media and internet companies, start ups, investors, regulators and governments in the UK and internationally.

Contents

Executive Summary

The Department for Digital, Culture, Media & Sport (DCMS) commissioned Spark Ninety to conduct an analysis of online advertising harms, the online advertising market and regulatory landscape. This analysis feeds into the Online Advertising Programme undertaken by the DCMS. This project was a limited exercise, based on desk research and interviews with the regulator and selected industry experts. Spark Ninety would like to thank these contributors, including the ASA, Confiant, White Bullet and Ebiquity. This project was conducted from February to April 2022.

Review of online advertising harms

There is a very wide range of ways in which online advertising can harm consumers and industry. The following taxonomy lists 15 categories of harmful advertising - and builds on the version presented in the DCMS Online Advertising Programme consultation[1]. These categories are not mutually exclusive: instances of harmful advertising may, for example, be both misleading and offensive; industry harms may also have an impact on consumers.

Table 1: Taxonomy of harms

Causes harm to:	Involves harmful ad:	Content is legal/illegal:	Category of harm
Consumers	Content	Illegal	Malicious advertising
			Fraudulent advertising, including scams - in many cases involving unsanctioned use of celebrity images
			Ads for illegal activities, products or services
			Counterfeiting
			Non-identified ads
			Misleading ads
		Legal	Offensive ads
			Ads for products or services deemed to be harmful, but not illegal
			Ads that are seen to contribute to body image concerns
	Targeting/placement	N/A	Mistargeting
			Discriminatory targeting
			Targeting vulnerable people
Industry	Content	Illegal	Ad fraud
	Placement	N/A	Brand safety (including mistargeting)
	Measurement		Inaccurate audience measurement

Malicious and fraudulent or scam advertising are the most serious threats at present, based on an assessment of the incidence of these categories of harms and the severity of the impact caused to individuals or businesses affected. 35,115 Action Fraud reports in 2020/21 were identified as being related to fraud enabled by online advertisements, based on keyword analysis[2]. The total estimated loss from

---

[1] DCMS, Online Advertising Programme consultation, 9 March 2022. Changes to this version include the addition of 'counterfeiting' as a separate category, and the incorporation of 'fake celebrity endorsement' within the category of fraudulent advertising.

[2] This data includes fraud initiated by paid-for advertising and non-paid for advertising such as organic search results and social media posts. Only fraud reports where victims self-reported relevant keywords (e.g. ads, pop up, banner) are counted, therefore this data is likely to underestimate the total number of reported frauds initiated by online advertising.

these reports was about £400 million[3]. Other categories of harm cause severe impacts for smaller numbers of people (such as advertising for illegal products and services) or mild impacts for large numbers of people (such as non-identified or inadequately disclosed social media advertising). Importantly, this assessment is relatively subjective: it is difficult to make like-for-like comparisons between different categories of harm due to a lack of consistent and comparable data and differences in the type of impact caused by harm, ranging from financial losses to exacerbation of mental health issues.

Table 2: Relative incidence and severity of consumer harms - indicative guide

	Low incidence[1]	Medium incidence[1]	High incidence[1]
High severity[2]		• Illegal products/ services [C]	• Malicious [C] • Fraud/scams [C]
Medium severity[2]	• Discriminatory targeting[3] [C] • Targeting vulnerable people[3] [C]	• Counterfeiting [C] • Harmful but legal [C] • Mistargeting [C] • Body image[3] [C] • Brand safety risk [I]	• Misleading [C] • Ad fraud [I]
Low severity[2]		• Offensive [C]	• Non-identified [C]

Key: [C] = Consumer harm   [I] = Industry harm. High threat - Low threat.

Notes: (1) Indicative guide to the relative incidence of harmful advertising in terms of the number of advertising impressions served to people. In absolute terms, the proportion of harmful advertising is low. See introduction section, below.
(2) Level of harm to an individual consumer or business. Subjective assessment e.g. it is difficult to compare financial losses with harm to well-being. The severity of impact of some harms can vary (e.g. misleading advertising may have a very low or high impact depending on the nature of the product or service advertised). The scale of industry harms are considered in the context of industry revenues (e.g. harms may be high in absolute terms, but low relative to a company's revenues).
(3) Highly uncertain due to very limited evidence about the incidence of harm.

These harms may occur on paid search, open display (publisher websites or apps), social media or classifieds advertising, or on social media influencer marketing. Certain harms are focused on certain parts of the market: ad fraud occurs primarily in the open display market[4], while non-identified advertising is found mainly in influencer marketing. Other categories such as misleading advertising are present across these forms of advertising.

Over the last two years, the landscape of harms has evolved. Complaints relating to social influencer advertising have increased, driven by strong growth in the amount of influencer marketing (see 'market trends' section, below): ASA complaint cases[5] grew 92% in 2021 to reach 3,662, accounting for 47% of all complaint cases relating to paid-for online advertising. 494 of these complaint cases (23%) resulted in an advice notice[6] or informal/formal investigation, with the remainder (77%) being outside the remit of the ASA or where the ASA determined that no breach of the advertising codes occurred and no further action was required.

---

[3] City of London Police / National Fraud Intelligence Bureau, Fraud Enabled by Online Adverts 2020/21 – Dip Sample report, November 2021. Involved analysis of Action Fraud reports. Quoted in the DCMS consultation on reviewing the regulatory framework for online advertising in the UK: The Online Advertising Programme - Impact Assessment.
[4] Refers to sales of fraudulent advertising inventory, such as non-human traffic. Search and social display advertising are relatively unaffected by this type of fraud because there are limited mechanisms for fraudsters to profit from non-human traffic.
[5] "Complaint cases" refers to specific adverts complained about to the ASA. Some adverts generate multiple complaints. Therefore the number of complaints received by the ASA exceeds the number of complaint cases.
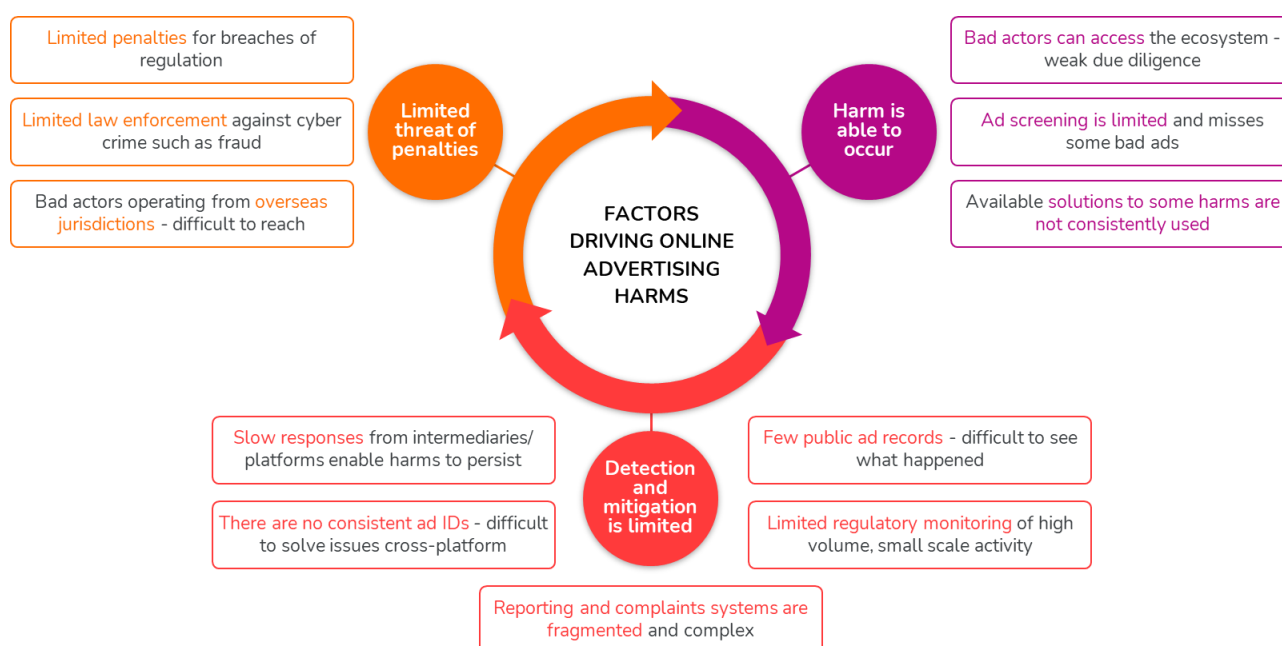[6] If the ASA decides that a possible breach of the Code has occurred but, on assessment against its prioritisation principles it is considered low priority, for example causing minor detriment, it will write to the advertiser explaining the issues and providing advice and guidance on how to comply with the Codes. It will not seek an assurance of compliance or contact the advertiser again regarding the matter.

Complaints about potentially harmful social display advertising also grew, with ASA complaint cases increasing 54% to 1,629, or 21% of all paid-for advertising cases. ASA complaint cases about open display advertising decreased 31% in 2021. However, according to data from security vendors, the volume of malicious and scam advertising (not generally counted in ASA case data) was up to 0.16% of UK programmatic advertising impressions in Q4 2021[7], while advertising verification vendors measured ad fraud (an industry issue outside the ASA's remit) at between 0.2% (mobile web) and 0.9% (desktop display) of UK impressions in H1 2021[8].

Anecdotal evidence suggests that the incidence of harms has decreased in certain narrow areas where the industry has strengthened consumer protection measures. Paid search advertising for investment scams appears to have decreased following the introduction of financial services advertiser verification by major platforms in August 2021[9]. Which? conducted a Bing search for 'compare best savings rates' on 20th September 2021, revealing adverts for 4 firms listed by the FCA as potentially harmful[10]. A Spark Ninety repeat of this search on Google and Bing on 20th March 2022 yielded no adverts for companies on the FCA's warning list, indicating a potential improvement.

Multiple factors contribute to the problem of harms, and these factors differ between categories of harm, supply chains (open display vs. owned and operated), and the organisations involved. Some factors contribute to the ease of harm happening in the first place, others contribute to limited detection and mitigation of harm after it has begun, and some limit the deterrent effect.

Figure 1: Factors contributing to online advertising harms - simplified

---

Market trends

The online advertising market is evolving at a fast pace. Online advertising expenditure is increasing, new advertising formats are emerging, and advertising practices are changing, especially around the use of data for targeting. Some of the main developments affecting online advertising harms include:

- Strong market growth, with pure play internet ad spend in the UK projected to reach £19.9bn by 2024[11], accounting for 72% of total advertising expenditure. Google, Meta and Amazon account for a growing market share, estimated at 80% to 90% of digital advertising globally outside of China[12].

- Outside of the major digital platforms, there is an increasing range of "publishers" with online advertising to sell, including games developers, audio streaming platforms, podcasters, connected TV platforms, online retailers, and social media "micro" and "nano" influencers.

- Online advertising formats are emerging that seamlessly integrate advertising into content and may present an elevated risk of inadequate identification of advertising. Examples include virtual billboards, virtual product placement and avatar sponsorship within games (and the metaverse in the longer term), and host-read advertising in podcasts.

- The influencer marketing industry is growing and evolving. Global expenditure is forecast to grow 19% year-on-year, from $13.8 billion (£10.6 billion) in 2021 to $16.4 billion (£12.6 billion) in 2022[13]. This is equivalent to about 3% of total global digital advertising expenditure in 2021. Brands are increasingly arranging paid promotions with micro- and nano-influencers (fewer than 40,000 followers) who may seem more authentic and credible and have stronger connections with their followers than big name influencers. This increases the number of influencers making paid-for posts. Influencer live streaming is also increasing and advertising in these streams is challenging to monitor where not recorded.

The online advertising industry is also moving away from certain privacy-invasive practices such as using third-party cookies to track users across websites and facilitate behavioural advertising. To a large extent, this move has been stimulated by web browsers withdrawing support for third-party cookies, and equivalent moves by mobile operating systems to limit access to mobile ad identifiers (MAIDs). There is growing use of alternative market practices, including contextual targeting, browser-based frameworks, data clean rooms, blockchain solutions and token-based advertising systems.

Supply chains

The programmatic open display and owned and operated advertising platform supply chains were described in the CMA online platforms and digital advertising report[14] published in 2020, which is to a large extent still valid as a generalised model. There are variations to this model, including the existence of an "alternative" programmatic open display advertising supply chain involving specialist intermediaries that serve adult content publishers and other restricted content publishers. Anecdotal evidence suggests that there is an elevated risk of harmful advertising in this supply chain. The ad tech intermediaries involved in the "alternative" supply chain are generally based overseas and are potentially challenging to regulate.

Recent trends in the programmatic open display advertising supply chain include a degree of simplification driven by limited market consolidation, growing vertical integration/alignment, supply path optimisation, and increased transparency (such as IAB standards sellers.json and SupplyChain Object[15] that allow buyers to see the sellers that intermediaries represent, creating a barrier to ad fraud).

---

[11] GroupM, This Year Next Year, UK End of Year Forecast, December 2020.
[12] https://www.thetimes.co.uk/article/uk-in-global-top-three-for-digital-advertising-t3f2kjtk6
[13] Influencer Marketing Hub and Refersion, Influencer Marketing Benchmark Report 2022
[14] CMA, Online platforms and digital advertising, Market study final report, 1 July 2020.
[15] https://iabtechlab.com/sellers-json/

Owned and operated platforms (e.g. Meta, Google, TikTok, Snap, Twitter) sell search and/or social display advertising on self-service interfaces, opening the market to large numbers of SME advertisers. Recently, platforms have tightened their ad safety measures and policies in certain limited areas and increased transparency, with developments including:

- Stronger advertiser on-boarding checks to prevent bad actors from advertising. Google recently introduced identity verification for all advertisers[16]. In 2021, Google, Meta, Microsoft, Amazon Ads, Twitter and Tiktok announced commitments to introduce requirements on financial services advertisers to demonstrate that they are authorised by the Financial Conduct Authority (FCA)[17]. Their timelines for implementing these requirements vary.

- Ad libraries to provide transparency. Meta Ad Library[18] now provides a public record of ads currently running on Facebook, Instagram, Messenger and Facebook Audience Network, but this does not include information about ad targeting. Google's new policies may enable it to introduce an ad library or similar transparency measures in the future[19].

- Ad targeting restrictions to prevent inappropriate targeting. In January 2022, Meta removed the ability for advertisers to target people based on certain sensitive data, such as health, race, ethnicity and political affiliation[20]. It also limits the targeting options available for people it knows to be under 18 to age, gender and location, with interest-based, lookalike and various other targeting disabled for this audience[21].

- Policies prohibiting certain forms of harmful advertising. Platforms have gone further than the requirements of the law and the CAP Code in banning some categories or types of advertising. For example, in August 2021 Twitter prohibited misleading 'before and after' photos, content that body shames a customer, and promotion of unhealthy or unsafe eating behaviours or eating disorders[22].

International policy developments

The regulatory framework for online advertising differs by country and is highly complex. In most cases, these frameworks involve consumer protection, data protection, media, communications, and vertical market laws as well as self-regulatory codes, and are enforced by government agencies and self-regulatory bodies. The main recent development among UK trading partners is the introduction of the European Union Digital Services Act (DSA) and Digital Markets Act (DMA). In April 2022, the time of writing, the text of these laws had been approved by the European Parliament, though there is the potential for changes during trilogue negotiations.

The DSA regulates intermediaries which they define as services that connect consumers with goods, services and content (e.g. internet service providers, cloud services, messaging, marketplaces and social networks). Specific obligations apply to online platforms (e.g. social networks, content-sharing platforms, app stores, online marketplaces, online travel and accommodation platforms) and a subset of rules apply to very large platforms (45 million or more users in the EU). Penalties will be set out in national laws, though the European Commission will have the power to impose fines on very large platforms of up to 6% of global turnover[23]. The main provisions of the DSA[24] for advertising include:

---

[16] https://support.google.com/adspolicy/answer/9720978?hl=en-GB&ref_topic=9646742

[17] https://www.techuk.org/resource/major-technology-companies-step-up-efforts-to-tackle-financial-fraud-and-scam-adverts.html

[18] https://www.facebook.com/ads/library/?active_status=all&ad_type=political_and_issue_ads&country=GB&media_type=all

[19] https://support.google.com/adspolicy/answer/9720978?hl=en-GB&ref_topic=9646742 Accessed 12 March 2022.

[20] https://www.nytimes.com/2021/11/09/technology/meta-facebook-ad-targeting.html

[21] https://www.facebook.com/business/help/229435355723442

[22] https://business.twitter.com/en/help/ads-policies/ads-policy-update-log.html

[23] https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348

[24] https://www.theregister.com/2022/01/22/eu_dsa_draft_meps/

- Transparency requirements. Online platforms must provide users with information about when and on whose behalf an advert is displayed, including who finances the advert, and how it is targeted to them. Voluntary codes of conduct will be developed for other market participants (e.g. open display intermediaries). Very large platforms will need to provide searchable ad libraries including content, advertiser and targeting details.

- Targeting prohibitions. Targeting of vulnerable groups based on special category data is prohibited as is the use of personal data for the targeting of minors.

- Targeting consent withdrawal requirements. Online platforms must ensure that users can easily refuse or withdraw consent for targeting advertising. The use of "dark patterns" (exploiting cognitive biases to prompt users to reveal information they do not want to) is prohibited.

- Access to data and algorithms. Very large platforms must provide the regulator and the European Commission with access to data and algorithms to enable an assessment of their advertising systems' risks and harms.

The DMA introduces rules for platforms that act as gatekeepers (e.g. search, social networking, messaging, operating systems, online intermediation) with an annual turnover in the European Economic Area of €6.5 billion or more[25] and with more than 45 million monthly active end users[26] in the EU. Penalties for non-compliance with the DMA include fines of up to 10% of the company's total worldwide annual turnover. Its main provisions[27] for advertising include:

- Requiring provision of pricing transparency information relating to the programmatic supply chain. Gatekeepers must provide advertisers and publishers to whom they supply services with free information about the price paid for each of the different advertising services provided.

- Banning intermediary gatekeepers from using business users' advertising data to then compete with them.

- Requiring access to performance measurement tools and information to allow independent verification. Gatekeepers must provide advertisers with performance measuring tools and data to allow them to carry out their own independent verification of their advertising.

- Banning personalised targeting without clear, informed consent. Clear, explicit, renewed, informed consent needs to have been given to the gatekeeper in line with the GDPR.

These laws primarily affect search and social media platforms, not advertisers and publishers. Open display advertising intermediaries are covered by a voluntary transparency code, and other measures apply only where these intermediaries qualify as platforms or gatekeepers (e.g. Google, Meta, Amazon, Microsoft).

The self-regulatory system for advertising will co-exist with these new laws in EU Member States. There have been separate regulatory developments in certain countries to address specific online advertising harms, such as a law in Norway to make it illegal for influencers to share retouched photos of their body in promotional posts[28], and the introduction of the Responsible Influencer Certificate[29] by the ARPP, the self-regulatory body for advertising in France.

---

[25] Or a market capitalisation of at least €65 billion.

[26] And/or more than 10,000 yearly active business users established in the EU.

[27] Amendments adopted by the European Parliament on 15 December 2021 on the proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) (COM(2020)0842 – C9-0419/2020 – 2020/0374(COD))

[28] https://www.stortinget.no/no/Saker-og-publikasjoner/Vedtak/Beslutninger/Lovvedtak/2020-2021/vedtak-202021-146/

[29] https://www.arpp.org/certificat-influence-responsable-inscriptions/

Introduction

The Department for Digital, Culture, Media & Sport (DCMS) commissioned Spark Ninety to conduct an analysis of online advertising harms, the online advertising market and regulatory landscape. This analysis feeds into the Online Advertising Programme undertaken by the DCMS.

Scope of work

This project explores harms relating to paid-for online advertising in the UK, in line with the scope of the Online Advertising Programme. The objectives of this study are to provide:

- An updated assessment of the nature and scale of online advertising harms.

- An analysis of the online advertising market, including trends, supply chains (open display and owned and operated) and industry initiatives.

- A description of emerging international online advertising regulatory developments, focusing on the European Union and the United States.

This project was a limited exercise, comprising 6 weeks of work, therefore these areas have been explored at a relatively high level. The focus has been on describing recent developments, building on other work in this area including a Plum Consulting report commissioned by the DCMS in 2020[30] and the DCMS Online Advertising Programme consultation[31] published in March 2022.

Methodology

The findings in this document are based on limited desk-based research and analysis including:

- Review of news media, company websites and reports, and data and reports from government and regulatory agencies, companies, charities and other civil society organisations.

- Review of data from the Advertising Standards Authority (ASA) about complaints, cases, monitoring studies and the Scam Ads Alert System.

- Analysis of certain information provided to the DCMS as part of its engagement with government and industry stakeholders.

- Searches on Google and Bing to identify examples of harmful paid search advertising in certain relevant categories such as fraudulent advertising, counterfeiting and illegal products and services. These searches were done on a small scale using selected search terms, and do not represent a comprehensive review.

- Searches of Meta Ad Library[32] to identify examples of harmful social media advertising in certain relevant categories such as body image, counterfeiting and illegal products and services. These searches were done on a small scale using selected search terms, and do not represent a comprehensive review.

In addition, the study team conducted a small number of targeted interviews with government agencies and industry stakeholders, including the ASA, White Bullet, Confiant, Ebiquity and the Home Office. These interviews focused on exploring issues that are not well documented in the public domain, such as cyber crime and online advertising relating to people trafficking. The project was conducted from February to April 2022.

---

[30] Plum Consulting, Mapping online advertising issues, and the industry and regulatory initiatives aimed at addressing them, May 2020.

[31] DCMS, Online Advertising Programme consultation, 9 March 2022.

[32] https://www.facebook.com/ads/library/?active_status=all&ad_type=political_and_issue_ads&country=GB&media_type=all

Notes about ASA data

Multiple sections of this report include ASA data about complaint cases. Each complaint case represents an instance of an advert that the ASA receives a complaint (or complaints) about. Importantly:

- Not all complaint cases involve harm. In 2021, only 16% of complaint cases relating to paid-for online advertising resulted in an advice notice or formal/informal investigation, with 84% being outside the ASA's remit or where the ASA determined that no breach of the advertising codes occurred and no further action was required. (See Annex 2 for details of a breakdown of action taken).

- Consumers may be more likely to complain about some forms of potential harms than others, distorting the relative number of complaint cases by category.

- The ASA categorises complaint cases as misleading, harm/irresponsibility, offensive or miscellaneous/other. Certain categories of harm are not included in this data (e.g. industry harms such as ad fraud and brand safety risk) or are not counted separately (e.g. advertising contributing to body image concerns).

Caveats

There is very limited consistent and comparable data about the incidence of harms related to online advertising in the UK, or the growth of these harms. As a consequence, the analysis presented in this report pulls together various sources to provide a composite analysis of harms, but there is substantial uncertainty in some of the results.

This project covered a very broad scope: 15 different categories of online advertising harm across 4 different market segments (search, social display, open display, classifieds); and 27 measures proposed in the government's consultation. Therefore, the analysis of these harms and interventions is necessarily high level and focuses on certain known issues.

This project was conducted prior to and during the government's Online Advertising Programme consultation, which was open from 17th March 2022 to 1st June 2022. Therefore, the project team did not have access to responses to this consultation. New information is likely to have come to light since the completion of this report.

Disclaimer

This report has been produced by Spark Ninety Limited, a limited company registered in England and Wales with registered number 11248585, in accordance with an engagement agreement for professional services with the Department for Digital, Culture, Media & Sport. This report contains information about the online advertising market based on sources believed to be reliable. The information is not advice and should not be treated as such. To the fullest extent permitted by law, Spark Ninety Limited and its employees do not accept or assume any responsibility or liability in respect of this report, or decisions based on it, to any reader of the report. Should such readers choose to rely on this report, then they do so at their own risk. Any views or opinions expressed in this report are those of Spark Ninety.

Review of Online Advertising Harms

Taxonomy of harms

There is a very wide range of ways in which online advertising can harm consumers and industry. The following taxonomy describes 15 categories of harmful advertising. These categories are not mutually exclusive: instances of harmful advertising may, for example, be both misleading and offensive; industry harms may also have an impact on consumers.

Table 3: Taxonomy of harms

Consumer/ industry	Content/ targeting	Legal / illegal	Category of harm
Consumer harms	Harmful ad content	Illegal harms	Malicious advertising
			Fraudulent advertising, including scams - in many cases involving unsanctioned use of celebrity images
			Ads for illegal activities, products or services
			Counterfeiting
			Non-identified ads
			Misleading ads
		Illegal harms	Offensive ads
			Ads for products or services deemed to be harmful, but not illegal
			Ads that are seen to contribute to body image concerns
	Harmful ad targeting and placement		Mistargeting
			Discriminatory targeting
			Targeting vulnerable people
Industry harms			Ad fraud
			Brand safety (including mistargeting)
			Inaccurate audience measurement

This taxonomy includes the following minor changes relative to the version published in the DCMS Online Advertising Programme consultation[33]:

● Counterfeiting is added as a separate category due to the specific characteristics of this IP crime compared to advertising of other illegal products, services and activities.

● 'Fake celebrity endorsement' is now included within 'Fraudulent advertising' because this harm is generally associated with scam advertising. It now refers to 'unsanctioned use of celebrity images' because some use of images is as sensational clickbait not endorsement.

Annex 1 provides a detailed description of each of these categories of harm, including examples, and an assessment of the nature, scale and severity of the harm.

---

[33] DCMS, Online Advertising Programme consultation, 9 March 2022.

Incidence and severity of harms

Malicious and fraudulent or scam advertising are likely to be the most significant harms in terms of frequency and severity of impact on people. Misleading advertising, counterfeiting, mistargeting, illegal products and services, and harmful but legal advertising follow in terms of overall impact. This assessment is relatively subjective due to the difficulty of making like-for-like comparisons between different categories of harm. This is a consequence of:

- Different measures of the incidence of harm being available for different categories of harm.

- Differences in the type of impact on individuals, ranging from financial losses to exacerbation of mental health issues, and limited data about these impacts.

Table 4: Relative incidence and severity of consumer harms - indicative guide

	Low incidence[1]	Medium incidence[1]	High incidence[1]
High severity[2]		• Illegal products/ services [C]	• Malicious [C] • Fraud/scams [C]
Medium severity[2]	• Discriminatory targeting[3] [C] • Targeting vulnerable people[3] [C]	• Counterfeiting [C] • Harmful but legal [C] • Mistargeting [C] • Body image[3] [C] • Brand safety risk [I]	• Misleading [C] • Ad fraud [I]
Low severity[2]		• Offensive [C]	• Non-identified [C]

Key: [C] = Consumer harm   [I] = Industry harm. High threat - Low threat.

Notes: (1) Indicative guide to the relative incidence of harmful advertising in terms of the number of advertising impressions served to people. In absolute terms, the proportion of harmful advertising is low. See below.
(2) Level of harm to an individual consumer or business. Subjective assessment e.g. it is difficult to compare financial losses with harm to well-being. The severity of impact of some harms can vary (e.g. misleading advertising may have a very low or high impact depending on the nature of the product or service advertised). The scale of industry harms are considered in the context of industry revenues (e.g. harms may be high in absolute terms, but low relative to a company's revenues).
(3) Highly uncertain due to very limited evidence about the incidence of harm.

Over the last two years, the landscape of harms has evolved. Complaints relating to social influencer advertising have increased, driven by strong growth in the amount of influencer marketing (see 'market trends' section, below): ASA complaint cases[34] grew 92% in 2021 to reach 3,662, accounting for 47% of all complaint cases relating to paid-for online advertising. 494 of these complaint cases (23%) resulted in an advice notice or informal/formal investigation, with the remainder (77%) being outside the remit of the ASA or where the ASA determined that no breach of the advertising codes occurred and no further action was required.

Complaints about potentially harmful social display advertising also grew, with ASA complaint cases increasing 54% to 1,629, or 21% of all paid-for advertising cases. ASA complaint cases about open display advertising decreased 31% in 2021. However, according to data from security vendors, the volume of malicious and scam advertising (not generally counted in ASA case data) was up to 0.16% of UK programmatic advertising impressions in Q4 2021[35], while advertising verification vendors measured ad

---

[34] "Complaint cases" refers to specific adverts complained about to the ASA. Some adverts generate multiple complaints. Therefore the number of complaints received by the ASA exceeds the number of complaint cases.

[35] Proportion of impressions that involve malicious clickbait, forced redirects, criminal scams and other dangerous activity. Source: Confiant, Malvertising and Ad Quality Index, Q4 2021.

fraud (an industry issue outside the ASA's remit) at between 0.2% (mobile web) and 0.9% (desktop display) of UK impressions in H1 2021[36].

The rating of the relative incidence of harms is based on the following assessment which takes into account different categories of available data to build a composite picture. **Importantly, these categories show different quantities which are not directly comparable**: the number of examples gives a broad indication of the number of publicly reported or findable instances of harmful advertising, while the percentage of ads served shows the proportion of open display advertising (a subset of the online advertising market) impressions or content that are harmful. **The overall assessment based on these measures provides a broad guide to the relative incidence of harmful advertising** in terms of the number of advertising impressions served to people. **The proportion of advertising impressions that is harmful appears to be low in absolute terms** (e.g. less than 1% in the case of ad fraud). It is not possible to provide a robust assessment of relative or absolute levels of harm due to the lack of consistent and comparable data across the different categories of harm.

Table 5: Relative incidence of harms - highly indicative guide

Category of harm	Number of examples [1]	% of ads served [2]	% of people exposed [3]	Number of ASA complaint cases [4]	Overall assessment of relative incidence [5]
Malicious advertising	Medium	0.16%[H]	n/a	n/a	**High**
Fraudulent advertising, including scams	High	<0.16%[6][H]	<17%[7][H]	n/a	**High**
Ads for illegal activities, products or services	Medium	n/a	n/a	n/a	**Medium**
Counterfeiting ads	Medium	n/a	9%-10%[8][M]	n/a	**Medium**
Non-identified ads	High	n/a	n/a	3,541[9][H]	**High**
Misleading ads	High	n/a	<27%[10][H]	6,364[H]	**High**
Offensive ads	Medium	n/a	n/a	454[M]	**Medium**
Harmful, but not illegal ads	Medium	n/a	n/a	956[M]	**Medium**
Ads contributing to body image concerns	Medium	n/a	n/a	n/a	**Medium ***
Mistargeting	Medium	n/a	n/a	n/a	**Medium**
Discriminatory targeting	Low	n/a	n/a	n/a	**Low ***
Targeting vulnerable people	Low	n/a	n/a	n/a	**Low ***
Ad fraud	High	0.2%-0.9%[11][H]	n/a	n/a	**High**
Brand safety risk	Medium	0.1%[12][M]	n/a	n/a	**Medium**

Key: [L]/Low - [M]/Medium - [H]/High. *** = High level of uncertainty due to very limited data.**

Notes: (1) Number of examples = indicative measure based on the frequency of media reports and other public reports of harms, and the number of examples found in a small number of selected searches on Google and Bing and on Meta Ad Library (see methodology section, above).
(2) % of ads served = proportion of ads in the programmatic open display market that cyber security or verification providers have measured. Excludes non-detected issues. Excludes social media, where relevant.
(3) % of people exposed = proportion of people who claim, in surveys, to have seen relevant categories of harmful advertising. In some cases, consumers are responding to broadly phrased questions that capture organic, non-paid for advertising as well as paid-for advertising.
(4) Number of ASA complaint cases in 2021. Importantly, **the number of ASA complaint cases is not a direct measure of the level of harm** because (a) consumers might be more likely to complain about some forms of harm than others, and (b) **not all ASA complaint cases involve harm**: only 16% of complaint cases relating to paid-for online advertising resulted in

---

[36] Average optimised-against-ad fraud levels. Source: IAS, Media Quality Report, H1 2021.

an advice notice or formal/informal investigation, with 84% being outside the ASA's remit or where the ASA determined that no breach of the advertising codes occurred and no further action was required.

(5) **The overall assessment refers to the relative incidence of harmful advertising i.e. the amount of harmful advertising impressions served to people relative to other categories of harmful advertising.** It is not a measure of the absolute proportion of advertising impressions that are harmful, which in most cases appears to be low (e.g. less than 1% in the case of ad fraud).

(6) Proportion of impressions that involve malicious clickbait, forced redirects, criminal scams and other dangerous activity. Source: Confiant, Malvertising and Ad Quality Index, Q4 2021.

(7) 17% of people claimed to have been targeted by a scam on social media (Which, November 2021) - likely to include paid and organic advertising. Excludes search, open display and classifieds.

(8) 9% of EU consumers have been duped into buying counterfeit goods by online advertising, and 10% of UK female consumers were prompted by social media endorsements to buy counterfeits. Source: European Union Intellectual Property Office, European Citizens and Intellectual Property report, 2020.

(9) Non-identified or inadequately disclosed adverts are a substantial subset of the 3,541 complaint cases of misleading influencer marketing.

(10) 27% of UK consumers claim to have seen misleading or harmful advertising on video sharing platforms. Excludes other social media, open display, search and classifieds. Source: Ofcom Video-sharing platform usage & experience of harms survey 2021.

(11) Proportion of UK programmatic advertising impressions that were fraudulent in H1 2021 ranged from 0.2% (mobile web) to 0.9% (desktop display) - after optimisation against ad fraud. Source: IAS, Media Quality Report, H1 2021.

(12) Proportion of UK open web content that was categorised as 'high' or 'very high' risk in H1 2021. Source: IAS, Media Quality Report, H1 2021

(12) Inaccurate audience measurement is not included on the table because this harm is not measurable on comparable metrics to other harms.

The rating of the severity of harms is based on a qualitative assessment of the impact of harms on people and industry.

Table 6: Relative severity of harms

Low	Medium	High
• **Offensive** advertising (offence to individuals) [C] • **Non-identified** advertising (misleading) [C]	• **Counterfeiting** (financial losses to businesses, individual harm from dangerous products) [C] • **Harmful but legal** (wide range of different harms e.g. exposure to legal drugs) [C] • **Mistargeting** (harm to minors from age-inappropriate ads) [C] • **Body image** (harm to mental health) [C] • **Misleading** (harm from products / services being other than described) [C] • **Ad fraud** (financial losses to advertisers) [I] • **Brand safety risk** (damage to companies' brand image, societal harm from funding piracy or other harmful content) [I] • **Discriminatory targeting** (exclusion of certain groups from opportunities) [C] • **Targeting vulnerable people** (exacerbation of other harms e.g. mental health) [C]	• **Fraudulent advertising, including scams** (substantial individual financial losses; damage to celebrity reputation in clickbait cases; damage to brand reputation in cloning cases) [C] • **Malicious advertising** (individual financial losses from theft of data and misappropriation of computer resources) [C] • **Illegal products and services** (individual harm from the purchase of illegal products or provision of illegal services e.g. people trafficking) [C]

Key: [C] = Consumer harm   [I] = Industry harm

Notes: (1) Level of harm to an individual consumer or business.

Trends in harms

There is very limited evidence about whether the scale of different harms has increased or decreased over the past 1-2 years because many data sources provide snapshots, not a time series, and the types of data available for each harm differ. The following table shows the trends in terms of anecdotal evidence (e.g. industry commentary), measured incidence (e.g. monitoring of advertising), ASA complaint cases, and estimated costs (e.g. economic costs) where available, and an overall composite assessment. In many cases, the available data does not point to a clear trend or relates only to a subset of the category of harm. Therefore, this assessment provides a top-level view: trends in some harms differ by category of advertising (e.g. search, social, open display) which is explored in the sections on each harm, below. Note that the number of ASA complaint cases is not a direct measure of the level of harm because (a) consumers might be more likely to complain about some forms of harm than others, and (b) not all adverts that they complain about are harmful. Therefore, this metric provides only a rough indication of potential changes in the level of harm.

Table 7: Trends in the scale of harms

Category of harm	Anecdotal reports	Measured incidence	Number of ASA complaint cases	Estimated cost	Overall assessment
Malicious advertising	⇨	⇧	n/a	n/a	⇨
Fraudulent advertising, including scams	⇨	⇧	n/a	⇧	⇧
Ads for illegal activities, products or services	⇨	n/a	n/a	n/a	⇨
Counterfeiting ads	⇨	n/a	n/a	n/a	⇨
Non-identified ads	⇧	n/a	⇧	n/a	⇧
Misleading ads	⇧	n/a	⇧	n/a	⇧
Offensive ads	⇧	n/a	⇧	n/a	⇧
Harmful, but not illegal ads	⇧	n/a	⇧	n/a	⇧
Ads contributing to body image concerns	n/a	n/a	n/a	n/a	n/a
Mistargeting	⇩	⇩	⇧	n/a	⇩
Discriminatory targeting	n/a	n/a	n/a	n/a	n/a
Targeting vulnerable people	n/a	n/a	n/a	n/a	n/a
Ad fraud	⇨	⇩	n/a	⇩	⇨
Brand safety risk	⇨	⇩	n/a	n/a	⇨

Key: ⇧ = Increase ⇩ = Decrease ⇨ = No change

At a more granular level, evidence is emerging that the incidence of harms has decreased in certain narrow sub-categories where the industry has strengthened consumer protection measures. Anecdotal evidence suggests that the incidence of paid search advertising for investment scams has decreased following the introduction of financial services advertiser verification by major platforms in 2021. Which? conducted a Bing search for 'compare best savings rates' on 20th September 2021, revealing adverts for 4 firms listed by the FCA as potentially harmful[37]. A Spark Ninety repeat of this search on Google and Bing on 20th

---

[37] https://www.which.co.uk/news/2021/10/fake-ads-rife-on-bing-as-investment-scams-jump-84/.

March 2022 yielded no adverts for companies on the FCA's warning list, indicating a potential improvement.

Causes of harms

Multiple factors contribute to the problem of harms, and these factors differ between categories of harm, supply chains (open display vs. owned and operated), and the organisations involved. Some factors contribute to the ease of harm happening in the first place, others contribute to limited detection and mitigation of harm after it has begun, and some limit the deterrent effect.

Factors contributing to the enablement of harms or the lack of prevention of harm taking place at source include:

- **Bad actor access.** Platform and intermediary customer due diligence procedures do not, in some cases, prevent bad actors, such as organised crime groups, from setting up accounts to buy advertising (e.g. scam advertising) or sell advertising (e.g. piracy services on which advertising may be misplaced).

- **Limited ad screening.** Platform and intermediary checks on ad creative and landing pages, up front and in flight (during a live campaign), do not detect all advertising that is in breach of their policies. This is a problem where harms in the advertising should be identifiable, such as unsanctioned use of celebrity images or fake URLs in the case of clone fraud.

- **Solutions not used.** In some cases, advertisers, intermediaries or platforms do not use available technology, data and services to limit harms. This may include use of standards for transparency in the open display supply chain (e.g. buyers.json) or use of data sources to identify harmful publisher content and prevent ad placement there.

Factors contributing to a lack of detection of harm and a slow or limited response after detection, such as takedowns, include:

- **Few public ad records.** At present, only Meta provides a comprehensive and publicly accessible library of ads on its platforms, though this is limited to certain information about live ads. Therefore, it is difficult for the public/stakeholders to know what ads are running and determine whether these are inappropriate.

- **Limited monitoring.** There is limited independent regulatory or law enforcement monitoring to detect harmful advertising or harmful activity such as ad fraud. Monitoring high volumes of small-scale ad campaigns (e.g. the long tail of micro-influencers, SME advertisers) is especially challenging.

- **Reporting issues.** The systems available for consumers to report inappropriate advertising are relatively complex and fragmented and, in some cases, rely on consumers to capture information about ads. Therefore, some harmful ads go unreported or reports are not investigated easily or swiftly.

- **Lack of ad IDs.** There is no commonly agreed identifier of ads - a creative ID. Different market participants identify creative copy in different ways. Therefore, when harmful advertising is identified on one platform or intermediary, it may be difficult to find instances of the same ad on other platforms.

- **Slow responses.** In some cases, intermediaries, platforms or publishers may be slow to respond to public, regulator or peer reports of harmful advertising or activity, and/or take limited action. As a consequence, harmful advertising or activity might continue after reports are received.

Factors contributing to a lack of incentive to comply with laws and regulations:

- **Limited penalties.** The penalties for breaches of the CAP Code or for breaking the law may be limited or, in the case of certain overseas advertisers or bad actors, unenforceable.

- **Limited enforcement.** Law enforcement in areas of cyber crime such as malicious advertising and ad fraud is relatively limited - in part due to the complexity of these offences. Therefore, bad actors might not believe that there is a strong prospect of investigation and conviction.

- **Overseas jurisdiction.** Some bad actors, such as cyber criminals responsible for malicious advertising and ad fraud, are based overseas. In consequence, investigation and prosecution may require international law enforcement cooperation which could be challenging to achieve in certain territories.

Figure 2: Factors contributing to online advertising harms - simplified
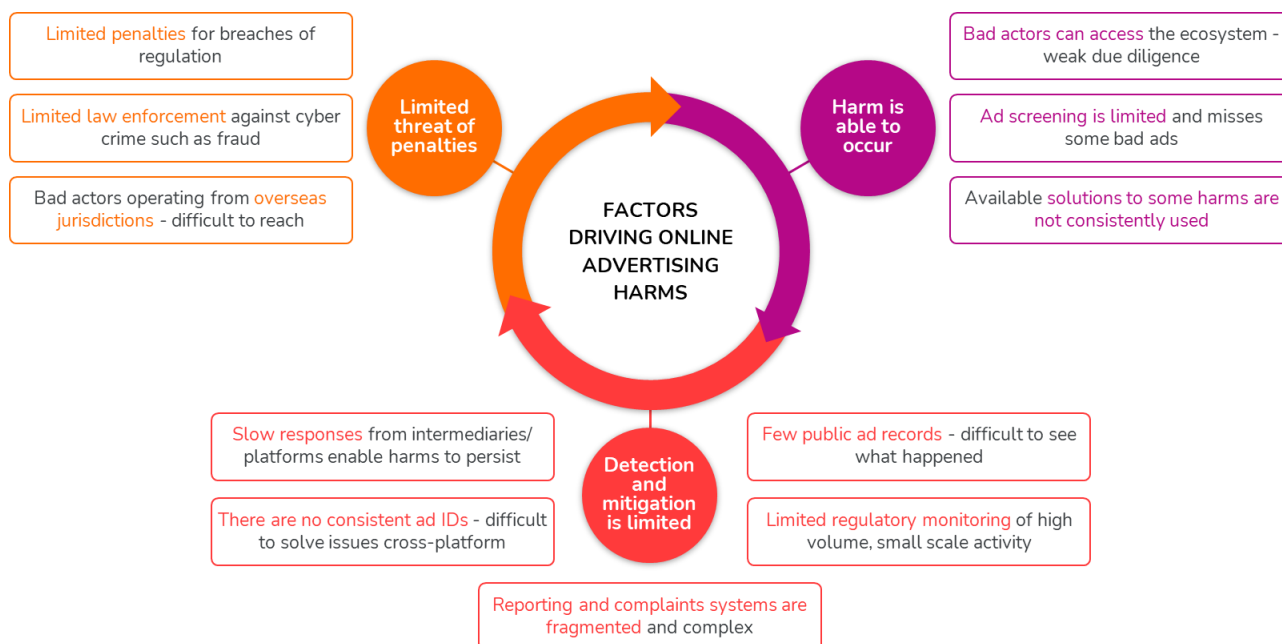
Table 8: Factors contributing to different categories of harm

Category of harm	Bad actor access [F]	Limited ad screening [F]	Solutions not used [F]	Few public ad records [D]	Limited monitoring [D]	Reporting issues [D]	Lack of ad IDs [D]	Slow responses [D]	Limited penalties [I]	Limited enforcement [I]	Overseas jurisdiction [I]
Malicious advertising	●	●		●	●	●	●	●		●	●
Fraudulent advertising, including scams	●	●		●	●	●	●	●		●	●
Ads for illegal activities, products or services	●	●		●	●	●	●				
Counterfeiting ads	●	●		●	●	●	●				
Non-identified ads					●	●	●		●		
Misleading ads		●		●	●	●	●		●		
Offensive ads		●		●	●	●	●		●		
Harmful, but not illegal ads		●		●	●	●	●		●		
Ads contributing to body image concerns		●		●	●	●	●		●		
Mistargeting			●	●	●				●		
Discriminatory targeting				●	●				●		
Targeting vulnerable people				●	●				●		
Ad fraud			●							●	●
Brand safety			●						●		
Inaccurate audience measurement											

Key: [F] = Factors enabling harm to occur   [D] = Factors limiting detection and mitigation   [I] = Factors limiting incentives to comply

Market Trends

The online advertising market is evolving at a fast pace. Online advertising expenditure is increasing, new advertising formats are emerging, and advertising practices are changing, especially around the use of data for targeting. The following section describes selected trends relevant to advertising harms. The scope of this project did not include a comprehensive review of the very large wider range of trends affecting the online advertising market.

Online advertising media and formats

The UK online advertising market is forecast to grow strongly over the next 3 years, with pure play internet ad spend projected to reach £19.9bn by 2024[38], accounting for 72% of total advertising expenditure. Search is forecast to continue to be the largest category, accounting for expenditure of £10.5bn by 2024, followed by display (£7.0bn, excluding news and magazine publishers and broadcasters), and e-commerce (£2.4bn). Google, Meta and Amazon account for a large market share, forecast to be 74% of digital advertising globally in 2022[39].

Figure 3: UK advertising revenues, 2012 to 2024
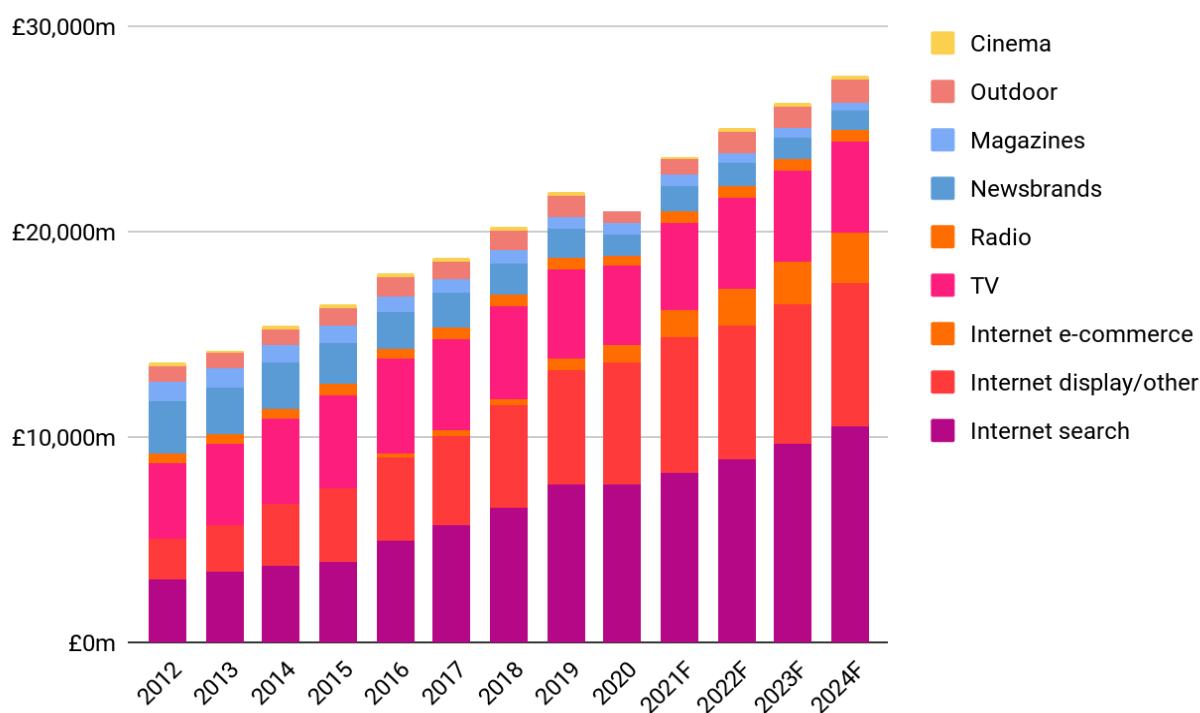
There is an increasing diversity of advertising media and formats, with growth across in-game, digital audio and connected TV advertising, retail media and influencer marketing. These developments have three main implications for online advertising harms:

● There is an increasing range of "publishers" with online advertising to sell, including games developers, audio streaming platforms, podcasters, connected TV platforms, online retailers, and social media "micro" and "nano" influencers.

---

[38] GroupM, This Year Next Year, UK End of Year Forecast, December 2020.
[39] Ebiquity, Google, Meta and Amazon are on track to absorb more than 50% of all ad money in 2022, February 2022.

- Intermediaries are emerging that specialise in trading advertising inventory in some of these areas, such as podcast advertising networks and influencer marketing platforms.

- Some emerging advertising formats carry an elevated risk of harm, such as non-identified advertising in the case of in-game product placement, influencer marketing and host-read podcast advertising, where the advertising is relatively seamlessly integrated with the content.

Table 9: Online advertising market segmentation and selected trends

Market segment and subsegment	Selected trends
Search	Emergence of voice search, visual search, augmented reality search, such as Google Lens and Live View in Google Maps[40].
Social display	① **Growth of major platforms** and a fast pace of change in the social media market, with innovation in social media advertising formats.
Open display: Standard and native display	More engaging and interactive ad formats, such as "playable ads" that enable mobile users to preview or try out an app within the ad[41], and native video ads that live stream brand video (e.g. Teads InRead Live[42]).
Open display: Video and connected TV	② **Growth in connected TV advertising** expenditure, the emergence of display advertising on device interfaces and increasing role for gateway platforms.
Open display: Audio	③ **Growth in podcast advertising** and the emergence of actionable audio ads enabled by voice devices.
Open display: In-game advertising	④ **Growing range of ad formats integrated into gameplay**, in some cases ad served, such as virtual billboards, virtual product placement and avatar sponsorship.
Open display: Retail media	⑤ **Retailers selling advertising on their websites and apps** and, in some cases, using first-party data to buy advertising on third-party services.
Classifieds	Increasing use of transactional business models with platforms taking a share of revenue as an alternative or complement to charging for advertising.
Influencer marketing	⑥ **Growth in influencer live streaming, and micro and nano influencers.** Growth of influencer intermediaries.

Numbered trends above are elaborated on in the following sections.

---

[40] https://arvr.google.com/ar/
[41] https://vungle.com/resources/playable-ads/
[42] https://www.teads.com/viewable-outstream-teads-formats/

① Social media advertising

There is a very wide range of trends and developments affecting the social media advertising market - it is beyond the scope of this report to detail these in full. Overall, the major owned and operated platforms account for an increasing share of the market. Ebiquity estimates that Google, Meta and Amazon grew their share of the global digital advertising market from 67% in 2020 to 74% in 2022[43] (note that these figures include search and open display advertising revenues as well as social).

There is a fast pace of change in the social media market in terms of advertising expenditure, formats and practices. For example, it is expected that TikTok will reach 1.5 billion monthly active users globally in 2022, with advertising revenues forecast to grow from $4 billion in 2021 to $12 billion in 2022[44]. This is small relative to Meta's $115 billion global revenues in 2021[45].

TikTik also illustrates the development of new advertising formats, with offers for both brand and response advertisers. For example, advertisers that have set up TikTok shops can create video shopping ads[46] showing products that people can buy by tapping on a product card in the ad to take them through to a shop. TikTok is also testing live shopping ads where people can purchase products from a live streamed ad[47]. These ad formats are examples of the "shoppable advertising" trend, where social platforms provide brands with advertising as well as ecommerce capabilities.

② Connected TV advertising

The majority of UK households are equipped with connected TV (CTV) devices, such as smart TV sets, streaming devices (e.g. Amazon Fire TV, Roku), games consoles and operator set-top boxes (e.g. Freeview Play). In Q1 2021, 79% of households used their TV set to watch online or on-demand content, with 44% using apps on a smart TV set and 29% a streaming box or stick[48].

These devices provide internet connectivity enabling people to view video on demand (VOD) and video sharing platform (VSP) services on their TV sets, and supporting the following range of CTV advertising formats[49]:

- CTV advertising - advertising served in an internet-delivered video service viewed on a TV set (e.g. video ads on ITV Hub, All4 or YouTube viewed on a TV set)

- Addressable advertising on broadcast TV - addressable ads that replace broadcast ads, with ad insertion enabled by a CTV device (e.g. Sky AdSmart)

- Advertising in CTV device user interfaces - display, video or paid search advertising placed in the device user interfaces, such as its home screen, electronic-programme guide, or search results (e.g. Samsung First Screen Ads)

Globally, the CTV advertising revenue is forecast to grow from $16.6 billion (£12.7 billion) in 2021 to $32.6 billion (£25.1 billion) in 2026, a compound annual growth rate (CAGR) of 14%[50].

The CTV advertising supply chain is comparable to the display advertising supply chain, with the exception that operators of operating systems, devices and app stores play a role. Known as 'gateway platforms', these companies include Google, Roku, Amazon, Samsung and other device manufacturers. Gateway

---

[43] Ebiquity, Google, Meta and Amazon are on track to absorb more than 50% of all ad money in 2022, February 2022.

[44] https://www.emarketer.com/content/tiktok-triple-its-ad-revenue-this-year

[45] https://digiday.com/marketing/the-rundown-google-meta-and-amazon-are-on-track-to-absorb-more-than-50-of-all-ad-money-in-2022/?utm_medium=email&utm_campaign=digidaydis&utm_source=daily&utm_content=220204

[46] https://ads.tiktok.com/help/article?aid=10007856

[47] https://ads.tiktok.com/help/article?aid=10009169

[48] Ofcom Technology Tracker 2021.

[49] Spark Ninety, Connected TV advertising market dynamics, November 2020.

[50] GroupM, This Year Next Year: Global 2021 End-Of-Year Forecast

platforms are involved in the provision of data for targeting (e.g. viewing data) and the sale of advertising on user interfaces and some third-party video services.

Broadcasters pre-clear advertising on their VOD services, limiting the risk of harmful advertising. However, other market participants do not generally pre-clear ads, and in some cases sell advertising programmatically, creating a risk that inappropriate advertising will be placed on TV screens.

③ Digital audio advertising

Digital audio advertising expenditure in the UK increased 17% to reach £127 million in 2020[51]. It includes advertising in streamed audio services (e.g. radio, Spotify) and podcasts. Podcast advertising is an area of especially high growth, with US podcast ad spending forecast to increase 31% in 2022.

Digital audio advertising formats include spots, sponsorships and host-read advertising. Digital audio advertising is becoming more interactive, with startups such as AdTonos and Say It Now enabling people to action ads via smart speakers. For instance, listeners were able to book a test drive after hearing a car ad[52]. There is potential for brand safety harm in the case of sensitive topic podcasts, and non-identified advertising in the case of host-read advertising.

The digital audio supply chain is comparable to other display media, with sales channels including direct, owned and operated platforms (e.g. Spotify Ads) and programmatic.

④ In-game advertising

In 2020, 62% of UK adults were playing games on any device, with 92% of 16-24s playing games. Mobiles, consoles and computers were the devices used to play games by the largest proportions of people[53], with games played ranging from action, sports and role-playing, to puzzles and casinos. Some games carry advertising, with UK games advertising revenues estimated to have grown from £190m in 2015 to £286m in 2019[54]. Globally, the in-game advertising market is forecast to grow at a CAGR of 16% over the period 2021 to 2025[55].

In-game advertising involves an increasing range of formats and practices. The main potential issues with in-game advertising include:

- Non-identification of advertising where ads are seamlessly integrated into gameplay (e.g. virtual billboards, virtual product placement, virtual character sponsorship). Deals between brands and games publishers might not be transparent to players.

- Inappropriate advertising where advertising is traded programmatically. With the exception of standard display formats, in-game advertising has generally been placed via direct deals between brands and games publishers, ensuring publisher control over ad content. Future growth in programmatic trading of games advertising (e.g. programmatic sales of virtual billboards) might increase the risk that inappropriate advertising is placed within games. Exposure of child audiences to advertising in age-restricted categories is a particular risk due to the young audiences for games.

---

[51] IAB Europe, Adex benchmark 2020 study. Converted from Euros to GBP at rate of £1 = €1.12.
[52] https://voicebot.ai/2020/12/03/first-interactive-commercial-radio-ad-campaign-debuts-on-london-smart-speakers/
[53] Ofcom, Adults' Media Use and Attitudes report, 2020/21.
[54] Ofcom, Online Nation, 2020 Report, 24 June 2020.
[55] Technavio, In-Game Advertising Market by Platform and Geography - Forecast and Analysis 2021-2025, May 2021.

Table 10: Overview of in-game advertising formats and potential issues

Advertising format	Description
In-game display advertising	Banners, badges, video, interstitials and rewarded video formats that appear in app and web games.
Virtual billboards	Digital form of out-of-home advertising (billboards). Ad placement may be static (pre-agreed between games publishers and brands) or dynamic (inserted live by intermediaries such as Bidstack, Anzu and Admix). In some cases, brand logos are seamlessly integrated into gameplay (e.g. the Volkswagen logo appears on the floor of the fighting ring in the UFC 3 game[56]).
Virtual product placement	Virtual versions of branded products are placed within games for players to interact with. Products may be incorporated into games during development or made available through downloadable content packages in the case of wearable/usable in-game items (e.g. sponsored unlocks of customisable clothing, vehicles or themed maps). The Mario Kart 8 game included a free-to-download Mercedes content pack[57], while Louis Vuitton-designed custom 'skins' that could be worn by characters in League of Legends[58].
Virtual character/avatar sponsorship/ promotions	Virtual characters or avatars in games may be sponsored and/or promote products. For example, Alex Hunter, a character in the FIFA 18 console game for Playstation 4, signs a deal with Coca-Cola and shoots a commercial for them as part of the game[59].

Figure 4: Example: NHS COVID virtual billboard advertising in the Dirt Rally 2.0 game, facilitated by Bidstack[60]

---

[56] World Today News, Why in-game advertising (especially now) has so much potential, 15th August 2020.

[57] Business Insider, Nintendo Mercedes Benz DLC for Mario Kart 8 is Actually Kind of Depressing, August 2014.

[58] Washington Post, This is what Louis Vuitton looks like in League of Legends, 29th October 2019.

[59] Digiday, 'A whole new world': Coke has a sponsorship deal with a virtual soccer star in 'FIFA 18', September 2017.

[60] Source: https://www.bidstack.com/news/press/motorsport-com-codemasters-adds-coronavirus-message-into-dirt-rally-2-0/

Figure 5: Example: Subway virtual product placement in the Uncharted 3 game[61]

Figure 6: Example: Mercedes content pack in Mario Kart 8[62]

⑤ Retail media

A diverse array of retailers, from Amazon, Walmart and Tesco, to Uber Eats and Skyscanner, are selling advertising on their websites and apps and, in some cases, using first-party data to buy advertising on third-party services. Amazon generated advertising revenues of $31.2 billion (£24.0 billion) in 2021, with growth of 32% in Q4 2021[63]. Major US retailer Walmart reported advertising revenues of $2.1 billion in 2021[64]. US retail media ad spending is forecast to increase by 31.4% in 2022 and 26.2% in 2023, accounting for 19.3% of digital ad spending in 2023[65].

In the UK, Tesco has developed the Tesco Media & Insight Platform in partnership with dunnhumby[66]. This platform is powered by Tesco Clubcard data and offers a range of advertising formats on Tesco's digital properties, including banner ads, sponsored search results and creative solutions, such as competitions. It also enables advertisers to target their customers on third-party digital publisher sites, through programmatic advertising, as well as on Facebook. Tesco also provides a range of in-store advertising formats, such as digital signage and in-store radio, as well as direct mail and coupons. Other UK retailers,

---

[61] Source: https://whatculture.com/gaming/10-weirdest-product-placements-in-video-games?page=2#:~:text=Subway%20customers%20who%20bought%20specific,performing%20some%20death%2Ddefying%20escape.

[62] Source: http://e-aagh.net/2014/08/mario-mercedes-leads-new-mario-kart-8-dlc/

[63] https://www.emarketer.com/content/amazon-has-larger-advertising-business-than-youtube

[64] AdExchanger, Walmart Breaks Out Ad Business Revenue At $2.1 Billion And Details How Ads Power Its Retail Evolution, 18 February 2022.

[65] eMarketer, Why 2022 will be the year of retail media networks, 14 January 2022.

[66] https://www.dunnhumby.com/tesco-media-insight-platform/

such as Sainsbury's[67] and Boots[68], also offer advertising on their digital services. It is reported that ASOS plans to launch a programmatic advertising business[69].

The risk of inappropriate advertising on most retail media platforms is likely to be relatively low because retailers generally sell advertising to supplier brands (reputable companies) through direct relationships, in some cases over self-service platforms. An exception is platforms that sell to the long tail of smaller brands (e.g. Amazon), where a small minority of these brands might be less reputable companies that seek to place misleading advertising, for example.

⑥ Influencer marketing

The influencer marketing industry continues to grow strongly, with the global market forecast to increase from $13.8 billion (£10.6 billion) in 2021 to $16.4 billion (£12.6 billion) in 2022[70]. This is equivalent to about 3% of total global digital advertising expenditure in 2021[71]. Some of the main trends relevant to harms and regulation include:

- Live streaming. Influencers are increasingly live streaming content on platforms such as Twitch, Mixer and DLive, as well as Facebook Live, YouTube Live and IGTV (Instagram). Growth has been particularly explosive on Twitch, with an 83% year-on-year increase in viewership during the pandemic[72]. They may promote products and services directly and/or place advertising in graphics or text in a video feed. On some platforms, including Twitch, IGTV (Instagram) and Mixer, streams are not automatically recorded for later viewing, creating a challenge for regulators to investigate reports of breaches, although creators/influencers can manually configure the settings to record their live streams for later viewing if they choose to do so. The ASA offers specific advice on advertising in live streaming[73].

- Micro and nano influencers. Brands are increasingly using influencers with small followings who may seem more authentic and credible and have stronger connections with their followers than big name influencers[74]. Micro influencers have approximately 1,000 to 40,000 followers, while nano influencers have fewer than 1,000 followers, though definitions are not widely agreed on. The emergence of a large volume of small-scale influencers could present a challenge for regulators in terms of compliance monitoring.

- Influencer intermediaries. Globally, the number of influencer-related service offerings, such as platforms and agencies, increased 26% to 18,900 in 2021. Influencer marketing platforms raised over $800 million (£615 million) in funding in 2021[75] with notable raises including LTK, Grin, Mavrck, CreatorIQ and Tagger. In some cases companies are aggregating micro and nano influencers: Heartbeat[76] specialises in bringing promotional opportunities to Instagram and TikTok accounts with followers from as few as 500. The involvement of these agencies and platforms in the placement of influencer advertising could help to improve regulatory compliance by making advertisers and influencers more aware of the rules.

---

[67] https://www.research-live.com/article/news/sainsburys-launches-retail-media-platform/id/5077102
[68] https://www.boots-uk.com/about-boots-uk/company-information/boots-media-group/
[69] https://digiday.com/marketing/asos-programmatic-ads-business/
[70] Influencer Marketing Hub and Refersion, Influencer Marketing Benchmark Report 2022
[71] Calculated using GroupM data for total global digital advertising expenditure.
[72] Insider Intelligence, Livestream surges in popularity after pandemic, 1st January 2022.
[73] https://www.asa.org.uk/news/go-live-advertising-in-live-streaming.html
[74] Forbes, Influencer Marketing's Surprising Rise Of The 'Everyperson', 4 February 2021.
[75] Influencer Marketing Hub and Refersion, Influencer Marketing Benchmark Report 2022
[76] https://heartbeat.com

Online advertising data and targeting

Online advertising market practices are evolving as a consequence of increasing restrictions on user tracking and behavioural targeting. There is a move towards alternative targeting mechanisms, such as contextual advertising, which can be facilitated without structural change to the supply chain.

Limits on user tracking across websites and apps

The online advertising industry is beginning to transition away from certain privacy-invasive practices such as using third-party cookies to track users across websites and facilitate behavioural advertising. To a large extent, this move has been stimulated by certain web browsers withdrawing support for third-party cookies, and equivalent moves by mobile operating systems to limit access to mobile ad identifiers (MAIDs).

Table 11: Status of use tracking on the main web browsers and mobile platforms

Environment	Competitor	Status of third-party cookies and mobile identifiers
Web browsers	Chrome	Third-party cookies **will be phased out from late 2023**[77] - postponed from an original target date of January 2022 due to industry and regulatory concerns around the impact of this move on competition.
Web browsers	Safari	Third-party cookies have been **blocked as default** since the release of Safari 13.1 in 2020. This is part of Apple's Intelligent Tracking Prevention (ITP) privacy feature[78].
Web browsers	Firefox	Third-party cookies have been **blocked as default** since the introduction of Firefox's Enhanced Tracking Protection in 2019[79].
Mobile platforms	iOS (Apple)	Apple launched App Tracking Transparency (ATT) in an update to the iOS14 operating system released in April 2021[80]. ATT **requires apps to seek user opt-in for use of IDFA (Apple's mobile identifier)**, in effect limiting cross-app tracking on iPhones, given that a large proportion of users are unlikely to opt in.
Mobile platforms	Android (Google)	Google **will support Android AdID for at least two years**. However, in February 2022 Google announced the Privacy Sandbox on Android[81] - a multi-year initiative to limit sharing of user data with third parties and introduce more private advertising solutions that operate without cross-app identifiers, including Android AdID.

The deprecation of third-party cookies has affected competitors differently. Websites with logged in users, such as social media services and some news websites, are still able to use first-party cookies to track people within their properties and serve targeted advertising. However, these same services are no longer able to behaviourally target many users on their iOS apps. In consequence, it is estimated that Snap, Facebook, Twitter and YouTube lost revenue of $9.85bn in Q3 and Q4 2021[82].

---

[77] https://digiday.com/marketing/cheat-sheet-google-extends-cookie-execution-deadline-until-late-2023-will-pause-floc-testing-in-july/

[78] https://www.zdnet.com/article/apple-blocks-third-party-cookies-in-safari/

[79] https://blog.mozilla.org/en/products/firefox/firefox-now-available-with-enhanced-tracking-protection-by-default/

[80] https://techcrunch.com/2021/04/26/apples-app-tracking-transparency-feature-has-arrived-heres-what-you-need-to-know/

[81] https://blog.google/products/android/introducing-privacy-sandbox-android/

[82] https://www.ft.com/content/4c19e387-ee1a-41d8-8dd2-bc6c302ee58e

Development of alternative business models

Third-party cookies and mobile identifiers, where in use, play a wide role - enabling behavioural targeting across websites as well as supporting other key elements of the online display advertising ecosystem, including audience measurement, attribution, and reach and frequency management. The online advertising industry is developing new practices and business models to replace this range of functionality - it is not focused solely on new methods of targeting. It is also exploring solutions to long-running problems with the open display advertising ecosystem, such as a lack of transparency and accountability and a susceptibility to fraud, viewability and brand safety/suitability issues. Some of the main areas of development include:

- **Contextual targeting** - online content and environments are categorised according to theme, keywords, sentiment, emotion or other characteristics, creating data and taxonomies that advertisers can target. For example, an airline might target web pages relating to travel, foreign languages, international sports, weather, or other indicators that might suggest an interest in booking flights. Contextual advertising practices are evolving, with ad tech providers experimenting with artificial intelligence (AI) to understand the context of web pages or apps[83].

- **Browser based frameworks** - Chromium Privacy Sandbox[84] is developing a range of solutions to replace functionality currently enabled by cross-site tracking using third-party cookies. These solutions generally involve consumer browsers processing personal data to allocate users into broad, non-individually identifiable cohorts (e.g. interest groups) that the online advertising ecosystem can interact with via browser API calls. In January 2022, Google proposed an API named Topics that categorises users into a small number of broad interest groups such as fitness or travel[85].

- **Data clean rooms** - ad tech providers such as InfoSum have developed means of matching data from different industry participants while maintaining the anonymity and privacy of end users. Applications for these clean rooms include matching advertiser and publisher first-party data, enabling advertisers to target potential customers who are on their databases on publisher websites and apps. This approach allows advertisers to activate their first-party data, instead of targeting based on segments provided by ad tech intermediaries, which are in some cases derived from third-party data originating from user "surveillance".

- **Blockchain** - distributed ledger technology (DLT) can be used to generate a single record of online advertising transactions, limiting the possibility for intermediaries to take excess margins through hidden fees or for nefarious actors to pass off fake advertising impressions as premium publisher inventory. There is a proliferation of blockchain advertising startups, such as Finestra, Alkimi Exchange[86] and Constellation Hypergraph. Alkimi is developing a blockchain advertising exchange that applies decentralised finance (DeFi) solutions to online advertising auctions[87].

- **Token-based advertising systems** - privacy-first web browser Brave has developed its own system of online advertising. The browser blocks advertising served by websites, such as banner ads and outstream video. Instead, Brave sells its own advertising which it serves into browsers in the format of tab sponsored images or browser notifications[88]. The Brave rewards scheme[89] gives users Basic Attention Tokens (BAT)[90] in return for viewing ads, tracks which websites users devote their attention to, then distributes users' BAT to these websites in proportion to this attention, with 70% of Brave ad revenues distributed in this way.

---

[83] https://www.exchangewire.com/deep-dive/contextual-advertising-ais-answer-to-a-cookieless-world/

[84] https://www.chromium.org/Home/chromium-privacy/privacy-sandbox

[85] https://blog.google/products/chrome/get-know-new-topics-api-privacy-sandbox/

[86] https://alkimiexchange.com/

[87] https://www.exchangewire.com/blog/2021/08/12/untangling-the-web-qa-with-alkimi-exchange/

[88] https://brave.com/brave-ads/

[89] https://brave.com/brave-rewards/

[90] https://basicattentiontoken.org/

Supply Chains

The programmatic open display and owned and operated advertising platform supply chains were described in the CMA online platforms and digital advertising report[91] published in 2020. To a large extent, the findings of this report relating to supply chains are still valid. This section builds on this work by describing:

- Recent trends and developments, especially changes to the supply chain structure and market practices.

- Variations on the simplified and generalised model (e.g. in specific market segments) to illustrate the range of participants and roles involved in online advertising.

- An "alternative" programmatic open display market ecosystem which carries an elevated risk of harmful advertising.

- Role of market participants with respect to ad safety, including advertiser on-boarding, ad clearance and monitoring, and response to reports of harmful advertising.
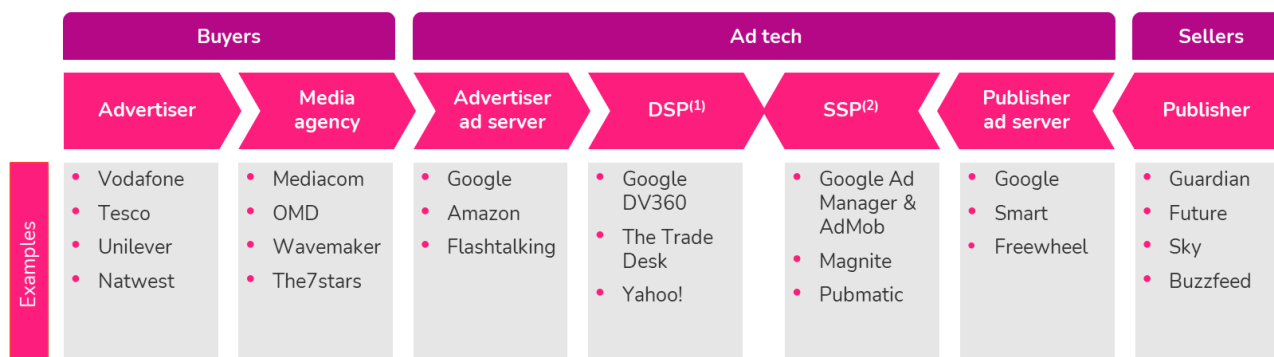
The Google (Google Ads and search), Meta, Snap and TikTok supply chains were selected by DCMS as a sample to illustrate the approaches of owned and operated platforms.

Open display market supply chain

Generalised supply chain

The following supply chain shows the ad tech participants generally involved in the trading and placement of online advertising sold programmatically by major publishers to major brands. This supply chain was described in the CMA Online platforms and digital advertising market study[92].

Figure 7: Programmatic open display advertising supply chain - simplified

Buyers		Ad tech				Sellers
Advertiser	Media agency	Advertiser ad server	DSP[(1)]	SSP[(2)]	Publisher ad server	Publisher
• Vodafone • Tesco • Unilever • Natwest	• Mediacom • OMD • Wavemaker • The7stars	• Google • Amazon • Flashtalking	• Google DV360 • The Trade Desk • Yahoo!	• Google Ad Manager & AdMob • Magnite • Pubmatic	• Google • Smart • Freewheel	• Guardian • Future • Sky • Buzzfeed

(Row label: Examples)

Notes:

1. DSP = demand-side platform.
2. SSP = supply-side platform.
3. Some ad tech competitors operate at multiple levels of the supply chain (e.g. Google, Amazon, Yahoo!).
4. This diagram simplifies the supply chain. Not all categories of ad tech vendors are shown, such as header bidding solutions and ad networks. In some cases, advertisers interface directly with ad tech vendors, without using a media agency. Some publishers sell ad inventory directly, involving manual orders or the use of an automated buying platform, without DSP and SSP involvement.
5. The ad tech ecosystem and roles are rapidly evolving.

---

[91] CMA, Online platforms and digital advertising, Market study final report, 1 July 2020.

[92] CMA, Online platforms and digital advertising market study - Appendix M: intermediation in open display advertising, 2020.

Participants in this supply chain include:

- Advertisers: Businesses and other organisations which direct the content of a message within an online advertisement, directly or indirectly, in order to influence choice, opinion, or behaviour.

- Media agencies: Typically major advertisers engage media agencies to provide strategic advice and plan and buy advertising on their behalf, though some advertisers have in-housed certain online media buying activities. Media agencies are generally part of holding companies that also include creative agencies and, increasingly, data propositions.

- Advertiser ad servers: Advertiser ad servers are used by advertisers and media agencies to store the ads, deliver them to publishers, keep track of this activity and assess the impact of their campaigns by tracking conversions.

- Demand-side platforms (DSP): Provide a platform that allows advertisers and media agencies to buy advertising inventory from many sources. DSPs bid on impressions based on the buyer's objectives and on data about the final user.

- Supply-side platforms (SSP): Provide the technology to automate the sale of digital inventory. They allow real-time auctions by connecting to multiple DSPs, collecting bids from them and performing the function of exchanges. They can also facilitate more direct deals between publishers and advertisers.

- Advertiser ad servers: Publisher ad servers manage the publisher's inventory and provide the decision logic underlying the final choice of which ad to serve.

- Publishers: Online publishers operate websites, apps or other online services and monetise their services by selling digital advertising. There is an increasing range of organisations in this category, including:

  - News publishers (e.g. The Guardian, The Telegraph, Reach)

  - Digital content publishers (e.g. Buzzfeed, Future)

  - Internet served Video-on-Demand (VOD) services (e.g. ITV, Channel 4, Pluto TV)

  - Audio publishers (e.g. Spotify, Global)

  - App developers (e.g. Tinder)

  - Games publishers (e.g. Activision, Epic)

  - Connected TV platforms (e.g. Roku, Samsung TV, Amazon Fire TV)

  - Retailers (e.g. Amazon, Tesco)

  - Other non-traditional publishers (e.g. Skyscanner, Uber Eats)

Variations on the generalised supply chain

In certain situations, the supply chain differs from the generalised programmatic model. Participants in the ad tech stack may be disintermediated or substituted by alternative categories of participant performing a similar role. The main variations include:

- **Direct sales.** Publishers may sell some online advertising direct to agencies or advertisers through:

  - Manual orders. Especially in the case of tenancies (where the advertiser pays a flat fee for a certain period of ad placement), custom solutions (e.g. non-standard advertising formats) and advertising sold as part of cross-platform packages (e.g. bundles of online and print advertising).

  - Owned and operated platforms. In certain cases, publishers have developed owned and operated self-service buying platforms that integrate the ad tech stack and avoid disintermediation by

third-party ad tech vendors. For example, ITV sells online video inventory through Planet V[93], a self service buying platform.

- **Ad networks.** The CMA defines ad networks as 'intermediaries that aggregate inventory supply from publishers and match it with demand from their own demand sources, therefore connecting advertisers and publishers and integrating in a single service most intermediation functions'[94]. The functions provided by ad networks are comparable to a combination of an ad server and an integrated SSP (e.g. Google AdSense, Google AdMob). In some cases, networks also integrate a DSP/self-service buying platform and/or conduct direct sales (e.g. Acast). Generally, ad networks serve small publishers or specific advertising formats, such as mobile, in-game and audio. Examples of ad networks include:

  - Google AdSense - used by small publishers to sell advertising through Google's own demand platform Google Ads as well as third-party DSPs.
  - Google AdMob - used by publishers to sell mobile app advertising inventory.
  - Acast - used by podcast creators to sell advertising in podcasts.

- **Self-service buying platforms.** Google Ads provides a buying platform for search and display advertising, including Google's display supply as well as third-party SSP supply. It integrates the functions of the advertiser ad server and DSP. Similarly, Facebook Ads Manager allows advertisers to buy advertising on Facebook Audience Network (publisher app inventory) as well as Facebook, Instagram and Messenger.

- **Agency disintermediation.** Some major advertisers have in-housed certain digital media buying activities, instead of agencies conducting these activities, or adopted hybrid models where advertisers and agency teams work together[95]. In many cases, SME advertisers buy online display advertising directly from self-service platforms such as Google Ads or Facebook Ads Manager without using an agency. The CMA estimated that around a quarter of all digital advertising expenditure in the UK is channelled through media agencies[96]. (The proportion of open display advertising expenditure channelled through media agencies is likely to be much higher than one quarter because this market segment has a lower weight of SME buyers than search or classifieds).

As a consequence of these variations, **an advertiser's point of entry into the open display advertising ecosystem could be a DSP, an ad network or a publisher - in some cases via a self-service platform.** A media agency may or may not be involved in this process.

Trends and developments

Although the open display advertising supply chain remains highly complex, it is becoming more simplified due to market consolidation, vertical integration/alignment, supply path optimisation, and increased transparency. Some of the main trends and developments since 2020 include:

- **Market consolidation.** The CMA estimated that in 2019 Google accounted for 50-60% of the value of ads sold across all of the SSPs and ad networks, with the remainder accounted for by Xandr, Teads, Taboola, Rubicon Project, Index Exchange and various others. Similarly, Google controlled 50-60% of the DSP market, with the remainder shared amongst The Trade Desk, Xandr, Criteo, Amazon and various others[97]. Recently, the long tail of competitors to Google has consolidated to a limited extent due to mergers and acquisitions. Major deals include:

  - In December 2021, Microsoft announced its acquisition of Xandr[98].

---

[93] https://www.planet-v.co.uk/

[94] CMA, Online platforms and digital advertising market study - Appendix M: intermediation in open display advertising, 2020.

[95] Digiday, Brands rethink their in-housing plans after tactic was 'put on ice' amid pandemic, April 2021 (behind paywall).

[96] CMA, Online platforms and digital advertising, Market study final report, 1 July 2020.

[97] CMA, Online platforms and digital advertising, Market study appendix C: Market outcomes, 1 July 2020.

[98] Microsoft Advertising Blog, Microsoft to acquire Xandr to accelerate delivery of digital advertising and retail media solutions.

- In December 2019, Rubicon Project and Telaria merged to form Magnite[99]. In April 2021, Magnite acquired Spotx[100].

- In September 2021, private equity firm Apollo Global Management acquired Verizon Media and renamed it Yahoo[101].

- **Vertical integration/alignment.** Programmatic open display advertising expenditure is increasingly following "closed" paths across supply and demand side intermediaries owned by the same companies. In many cases, major ad tech companies operate intermediaries at different levels of the supply chain (e.g. Google DV360/Google Ads - Google AdSense/Google Ad Manager/Google AdMob; Yahoo! DSP - Yahoo! SSP). IAB Europe analysed 5 companies and found that a high share of spend on their SSPs comes from their own demand (e.g. DSPs), with rates ranging from 35.3% to 94.1%[102]. It forecasts that the share of programmatic expenditure via the open ecosystem will decrease from 40.2% in 2021 to 25.3% in 2025.

- **Supply path optimisation (SPO).** Programmatic trading often involves multiple SSPs conducting parallel auctions for each ad impression, which creates duplication and inefficiencies. There is a growing trend towards finding the path from buyer to seller that is optimal in terms of fees and other factors - SPO. This trend is closely related to supply chain transparency, below. In some cases, SPO involves cutting out intermediaries: DSP The Trade Desk introduced OpenPath, a service that enables advertisers to access publisher ad inventory directly, bypassing SSPs (in cases where the publisher users Prebid, a header bidding solution)[103].

- **Supply chain transparency.** The IAB has introduced transparency standards. On the demand side, buyers.json and DemandChain Object[104] allow sellers to see the buyers that intermediaries represent. Conversely, on the sell side, sellers.json and SupplyChain Object[105] allow buyers to see the sellers that intermediaries represent. The online advertising industry is also making steps towards standardising supply chain audit procedures. A cross-industry task force involving ISBA, the IPA, IAB UK and the AOP have developed a strategy for achieving financial audit transparency for programmatic advertising[106]. This involves principles, an agreed data fields list, and a standard audit permission letter.

These trends are mainly relevant to programmatic trading of standard display advertising formats, such as banners, billboards and site skins. There is an increasing diversity of other online advertising formats, including video, audio, in-game and connected TV home screen advertising. In general, the supply chains for these market segments are comparable to the generalised display market supply chain. The main differences are the presence of specialist players (e.g. in-game advertising networks), category-specific ad tech (e.g. server-side ad insertion in video streaming), and a bias towards direct sales due to less developed programmatic trading.

---

[99] https://investor.rubiconproject.com/news-releases/news-release-details/rubicon-project-and-telaria-agree-combine-form-largest
[100] https://www.magnite.com/press/magnite-closes-spotx-acquisition/
[101] https://techcrunch.com/2021/09/01/apollo-completes-its-5b-acquisition-of-verizon-media-now-known-as-yahoo/
[102] IAB Europe, Economic Trends Forum Part 2, February 2022. Based on a review of SSP data from 12 publishers. This data is biased towards premium publishers.
[103] https://www.adexchanger.com/publishers/is-the-trade-desk-encroaching-on-ssp-turf-with-openpath/
[104] https://iabtechlab.com/buyers-json-demand-chain/
[105] https://iabtechlab.com/sellers-json/
[106] Videoweek, Industry Trade Groups Release New Tools to Crack Down on the Unknown Delta, 23 February 2022.

"Alternative" programmatic online advertising supply chain

Major online advertising intermediaries operate restrictions and prohibitions on content and advertising in certain categories. On the supply side, they generally apply advertising restrictions to content in sensitive categories, such as adult, recreational drugs and gambling. For example:

- Google Publisher Restrictions (across the Ad Manager, AdMob and AdSense SSP/networks) apply to sexual content, shocking content, and content relating to explosives, weapons, tobacco, recreational drugs, alcohol sale or misuse, online gambling, among other areas. Google Ads will not serve ads on this restricted content. Other demand sources (e.g. DSPs) could serve advertising on content labelled as restricted, but are likely to avoid it. Google states that publishers can choose to monetise content covered by these restrictions, but are likely to receive less advertising than other, non-restricted content[107].

- Major SSP Magnite applies "baseline content standards" that prohibit extreme content, including hateful supremacist speech, direct calls for violence or harassment, gratuitous depictions of violence, pornography, or materials that advocate illegal activities such as sexual abuse, fraud and piracy. It also prohibits harmful disinformation. It performs checks during publisher onboarding and monitors publisher content using third-party monitoring and classification services[108]. Therefore, it would be challenging for adult or piracy sites to monetise their services via Magnite.

On the demand side, they generally prohibit advertising for illegal content and services, such as copyright infringement, drugs and counterfeit goods and restrict advertising in areas such as alcohol and gambling. For example:

- Adform, a DSP and SSP, prohibits advertising that includes content across a range of categories including, but not limited to, hate speech, religion, pornography, weapons, copyright infringement, counerfeit goods and malware. Advertisers require Adform's written content to place ads in restricted categories, such as alcohol, gambling, financial services and politics. It requires advertisers to confirm that they comply with applicable laws and regulation in the country of the audience targeted[109].

- Google Ads and Google DV360 prohibit advertising of counterfeit goods and dangerous products, ads that enable dishonest behaviour or involve misrepresentation, inappropriate content such as accident images, and a wide range of other forms of content and product. It restricts ads that include sexual content, alcohol, gambling, politics, financial services, among other areas[110].

As a consequence of these restrictions publishers and advertisers operating in legal but restricted areas, especially adult entertainment, are to a large extent exiled from the mainstream display advertising ecosystem. Alternative ad tech vendors have emerged to service these exiles, leading to the creation of an "alternative" ecosystem. This ecosystem, illustrated above, is characterised by:

- Relatively large scale. The alternative ecosystem is likely to account for high volumes of online advertising inventory. Intermediary TrafficJunky specialises in dating, cannabis, adult entertainment, gambling, health & wellness and games publishers. It claims to process 218 million daily ad impressions in the UK[111].

- Fragmented market. There are multiple ad tech intermediaries that specialise in selling advertising for publishers in restricted content categories, especially adult entertainment.

---

[107] https://support.google.com/publisherpolicies/answer/10437795?visit_id=637824427002597315-4120494383&rd=1
[108] https://www.magnite.com/blog/on-content-standards/
[109] https://site.adform.com/policies/policies-and-guidelines/ad-quality-policies/
[110] https://support.google.com/adspolicy/answer/6008942
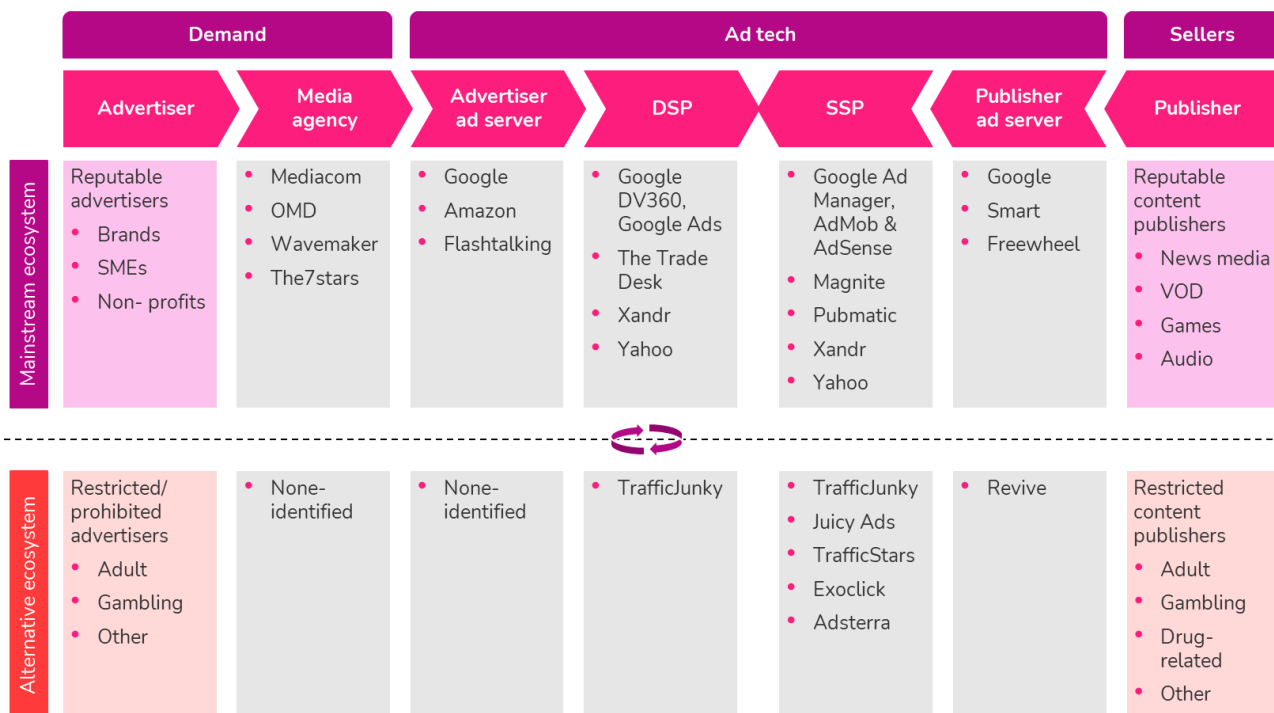[111] https://www.trafficjunky.com/online-advertising/traffic-statistics Accessed 10 March 2022.

- Variety of business models. Intermediary business models include SSPs, DSPs and networks, including affiliate networks. Some intermediaries integrate the full ad tech stack, providing advertisers with a self-service buying platform.

- Intermediaries based overseas. Major ad tech intermediaries operating in the alternative ecosystem are based overseas, such as Cyprus (TrafficJunky, Traffic Stars, Adsterra), Spain (ExoClick) and Canada (Juicy Ads).

The figure below illustrates this ecosystem. There is a degree of crossover between these ecosystems: for example, in some circumstances SSPs in the alternative ecosystem may sell some advertising to DSPs in the mainstream ecosystem.

Figure 8: Mainstream and "alternative" open display ecosystems - with examples of participants

| | Demand | | Ad tech | | | | Sellers |
	Advertiser	Media agency	Advertiser ad server	DSP	SSP	Publisher ad server	Publisher
Mainstream ecosystem	Reputable advertisers • Brands • SMEs • Non-profits	• Mediacom • OMD • Wavemaker • The7stars	• Google • Amazon • Flashtalking	• Google DV360, Google Ads • The Trade Desk • Xandr • Yahoo	• Google Ad Manager, AdMob & AdSense • Magnite • Pubmatic • Xandr • Yahoo	• Google • Smart • Freewheel	Reputable content publishers • News media • VOD • Games • Audio
Alternative ecosystem	Restricted/ prohibited advertisers • Adult • Gambling • Other	• None-identified	• None-identified	• TrafficJunky	• TrafficJunky • Juicy Ads • TrafficStars • Exoclick • Adsterra	• Revive	Restricted content publishers • Adult • Gambling • Drug-related • Other

The major intermediaries have policies prohibiting illegal advertising or content, such as Traffic Stars advertiser guidelines[112] and ExoClick compliance information[113]. However, anecdotal evidence suggests that the alternative ecosystem carries a relatively high level of harmful advertising.

- White Bullet research found that 16% of UK ad impressions on piracy websites were malware, fraud, or adult ads in Q1 2022, compared to 19% in 2021[114].

- In 2020 and 2021, adult entertainment websites were targeted by a malvertising campaign where the ads initiated redirects to fake Microsoft Windows system security alerts that were used to download malware[115].

---

[112] https://trafficstars.com/guidelines

[113] https://www.exoclick.com/compliance/

[114] White Bullet, How regulation and outreach reduce ad placement on piracy websites, 2022.

[115] https://blog.malwarebytes.com/cybercrime/2021/02/malvertising-campaign-on-top-adult-brands-exposes-users-to-tech-support-scams/

Owned and operated platform supply chains

Supply chain and the role of self-service platforms

The main social display and search platforms -Meta (Facebook, Instagram), Google (Google Ads, YouTube) TikTok, Snap and Twitter - have owned and operated supply chains. Their advertising businesses are built on scale and data, with each service reaching millions or tens of millions of logged-in users and gathering extensive first-party data. This enables them to offer advertisers a range of targeting strategies from laser pinpointing to mass market coverage, and options in between.

Search and social display platforms sell advertising on self-service interfaces, enabling a wide range of advertisers to buy advertising, including almost anyone with a registered business or other organisation, and in some cases individuals. This contrasts with some other media such as broadcast TV that have relatively high barriers to entry. TV advertising requires a budget of at least a few thousand pounds, a degree of advertising creative and production expertise, and compliance with a centralised advertising copy pre-clearance process (Clearcast).

These self-service buying platforms are part of a vertically integrated supply chain. Platforms also provide advertising inventory management and allocation, and tools and services such as dynamic content optimisation, data management, attribution and reporting, though offerings vary between providers. They also provide their consumer-facing services.

Figure 9: Owned and operated platform supply chain - simplified
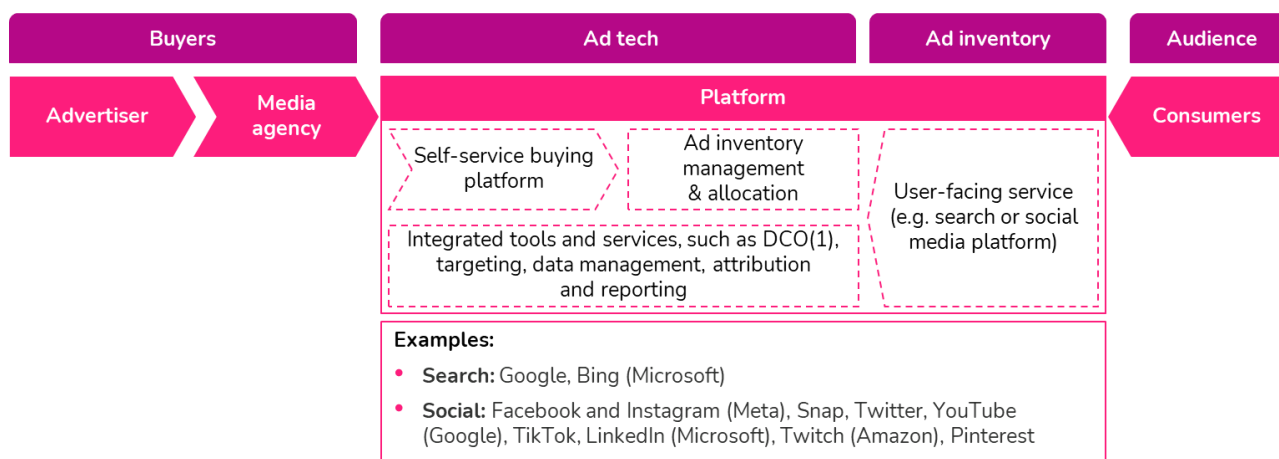
Notes:
(1) DCO = dynamic content optimisation.
(2) This diagram simplifies the supply chain. In some cases, advertisers interface directly with platforms, without using a media agency. In some cases, advertisers or media agencies use tools such as Smartly.io to manage campaigns on platforms. In some cases, publishers distribute content on platforms in return for a share of advertising revenue and/or the right to sell advertising on their content.
(3) Buying channels and platforms, and tools and services differ between platforms.

While this supply chain provides relatively unconstrained access to advertising, enabling small businesses to promote themselves and grow, it also puts creative and media buying decisions into the hands of thousands of individuals and small businesses, some of whom will be inexperienced, disinterested, uninformed and potentially lack diligence. To some extent, they require 'hand-holding' through the onboarding and advertising processes by providing clear language, navigation and guidance. Inevitably the low barriers to entry can, in some circumstances, also give those with malign intentions the opportunity to advertise too.

Ad safety procedures

Search and display advertising platforms and open display intermediaries have a range of policies and measures in place intended to protect consumers from harmful advertising. These measures follow the advertiser user journey from signing up with a platform (on-boarding) through to running advertising campaigns. These policies and procedures are constantly evolving - the following sections highlight recent developments.

Advertiser on-boarding checks

During customer on-boarding or thereafter, advertisers may be asked to verify their identity and/or that they are registered with relevant authorities. In most cases, vendors do not publish information about these 'know your customer' procedures and it is unclear whether and how any checks are performed. Some of the main developments since 2020 include:

- Specific vertical market requirements. Certain players have introduced financial services advertiser verification: advertisers must demonstrate that they are authorised by the Financial Conduct Authority (FCA). Google introduced this measure in August 2021, with Meta, Microsoft, Amazon Ads, Twitter and Tiktok also having committed to introducing comparable requirements[116]. (see next section).

- Advertiser identity verification. Google recently introduced identity verification and will make available 'ad disclosures' showing the advertiser name and location[117].

Generally, platforms require that advertisers set up business accounts and accept their general terms of service, community guidelines and privacy policies as a condition for access and use, providing grounds for suspension or removal of any advertising deemed to be in breach of their policies.

Ad reviews and approvals

Generally, platforms and DSPs review ads prior to delivery and in-flight (during a campaign) using in-house technology and teams or external vendors. Review typically involves an automated scan for malware (in the case of open display advertising) and other policy violations, with escalation to human review.

In the case of platforms, advertisers provide creative copy, target audience and other details on a self-service platform that are then checked and validated for publication. A mix of automated and human processes are deployed, and typical review times are around 24 hours[118]. Checks cover such aspects as the eligibility of the product/service; creative content and quality; the targeted region and age group; congruence between ad creative and landing page; and the functionality and eligibility of the landing page. Re-editing of creative copy or a change of target audience can trigger the review process again. Ads may be reviewed again after they are live for any reason.

Intermediaries and platforms do not publish information about how their ad reviews work. However, it is likely that the focus is on more serious and readily identifiable issues, such as malware, scams and IP infringement. It is unlikely that this process could detect more nuanced issues such as checking the veracity of advertiser claims in order to identify misleading advertising. In Meta's words, *'Reviewing ads from millions of advertisers globally against our Advertising Policies is essential, but it is not without challenges. Our enforcement isn't perfect, and both machines and people make mistakes.'[119]*

---

[116] https://www.techuk.org/resource/major-technology-companies-step-up-efforts-to-tackle-financial-fraud-and-scam-adverts.html
[117] https://support.google.com/adspolicy/answer/9720978?hl=en-GB&ref_topic=9646742
[118] Google Ads: Most ads are reviewed within a working day. Once deemed 'Eligible' an ad can run.
 TikTok: Most ads are reviewed within 24 hours.
Meta: Ad reviews are typically completed within 24 hours, primarily via automated tools
Twitter states: "Twitter Ads can be reviewed prior to running in campaigns. They are submitted for approval on an automatic basis, based on an account's advertising status, its historical use of Twitter, and other evolving factors. Review generally takes into consideration how an account uses Twitter, its profile, its content, and targeting included in any active or draft advertising campaigns."
Snap: "Most ads are reviewed within 24 hours, although depending on a variety of factors, it may take longer."
[119] https://www.facebook.com/business/help/204798856225114?id=649869995454285

If the validation process rejects an ad, then the buyer is given the reason(s) why and guided towards correcting the non-compliant content. Advertisers usually have the right of appeal if they regard a rejection as mistaken. In the case of serious or repeat offenders, platform policies allow for the suspension of advertising accounts, or even their permanent exclusion.

Figure 10: Example review process: Meta[120]
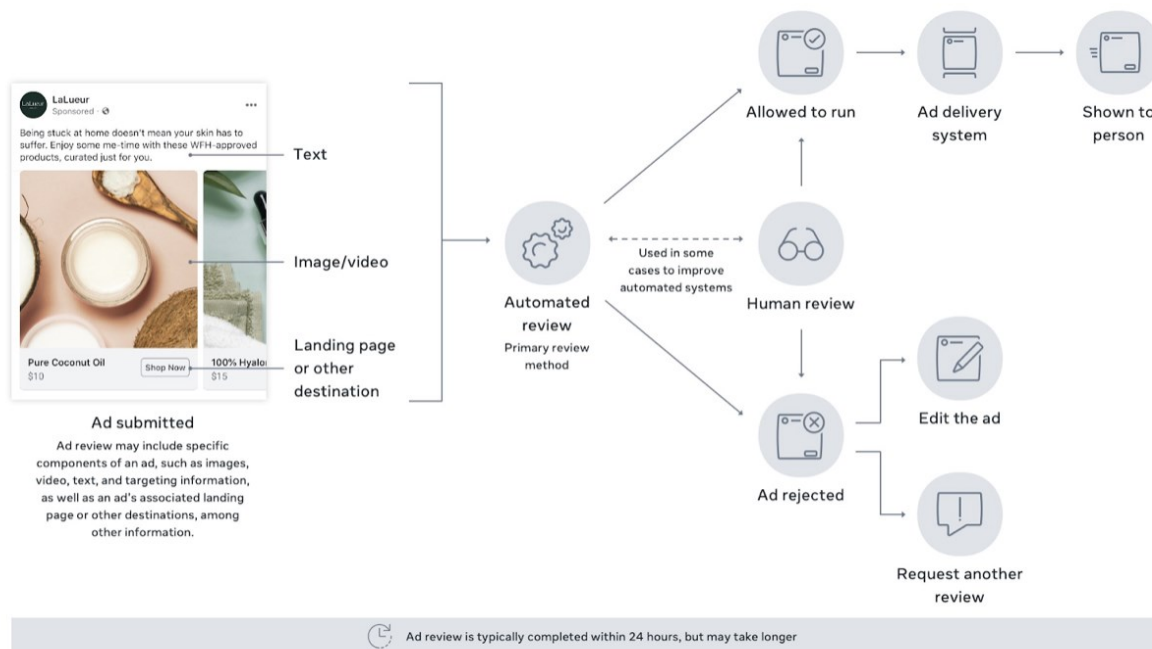
Ad safety review algorithms can inadvertently catch legitimate businesses with the parameters they use. The telehealth service Wisp, which connects clients with providers for care relating to sexual and reproductive health, has faced obstacles to advertising[121].

Ad targeting restrictions

Platforms offer advertisers various targeting options, such as demographics (gender, age), location, language, custom audiences, lookalike audiences, retargeted audiences, interests and behaviours, device and operating system. The self-service buying interfaces ask what is being advertised and allow the creation of a target audience based on the selection of such options, individually or in combination.

At the booking stage platforms impose exclusions or disable certain options to prevent some inappropriate targeting, such as advertising age-restricted products to children. For example, Meta advises advertisers of alcoholic drinks: *To ensure proper targeting, if you target an age group outside the legal directives, we'll automatically set the minimum age to the legally approved limit for the specific country/state and then approve the ad*. Similarly, for health and fitness advertisers: *If you're promoting health and fitness products and/or services, including vitamins and supplements, you must target your ads to people ages 18 and older. If you target your ad to people younger than 18, you'll be notified in Ads Manager that we've automatically set the minimum age to 18 so that it can be approved for delivery*.[122] These default settings and restrictions on the selectable audiences minimise the risk of mis-targeting.

---

[120] https://www.facebook.com/business/help/204798856225114?id=649869995454285
[121] https://www.adexchanger.com/digital-marketing-2/why-womens-health-is-hit-hardest-by-facebooks-ad-approval-algorithms/?oly_enc_id=6866E6018134F8Z
[122]
https://www.facebookblueprint.com/uploads/resource_courses/targets/393309/original/index.html?_courseId=187039#/page/5be3853da2488a7e42159af0

Figure 11: Meta audience selection interface[123]
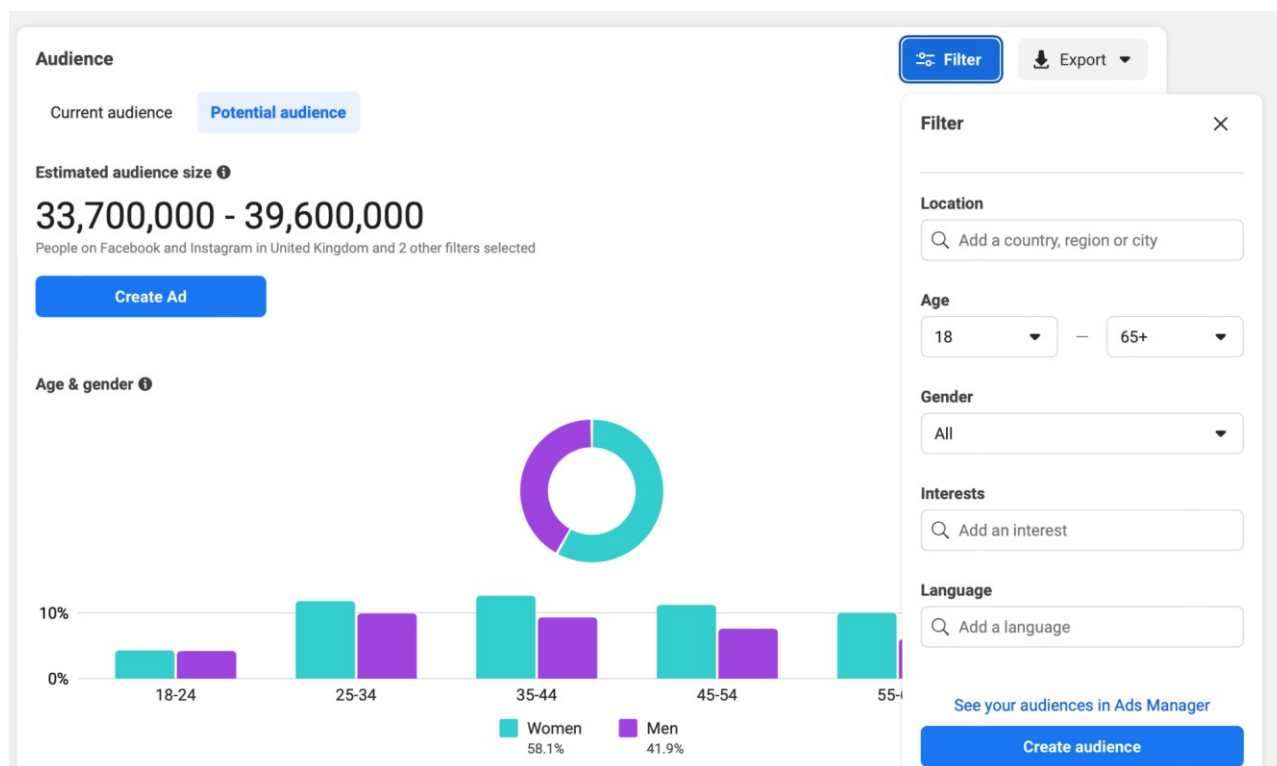
Ad libraries

Meta Ad Library[124] provides a public record of ads currently running on Facebook, Instagram, Messenger and Facebook Audience Network (which operates in the open display advertising market). The transparency provided by this library may help stakeholders to identify and notify Meta about harmful advertising. Snap[125] also has an ad library, but it is limited to political ads at present.

Open display advertising intermediaries do not currently operate comparable libraries, though Google's policies imply that it may introduce an ad library or similar transparency measures in the future: '*As Google expands its transparency efforts, we may make information about your Google Ads accounts and ad campaigns publicly available including: Advertiser name change history, Ad creatives, Dates and locations ads served...*'[126]

---

[123] Audience Insight section supporting the booking:
https://business.facebook.com/latest/insights/people?asset_id=114384364580285&nav_ref=audience_insights
[124] https://www.facebook.com/ads/library/?active_status=all&ad_type=political_and_issue_ads&country=GB&media_type=all
[125] https://www.snap.com/en-GB/political-ads
[126] https://support.google.com/adspolicy/answer/9720978?hl=en-GB&ref_topic=9646742 Accessed 12 March 2022.

Advertising policies

The major search and social media platforms and open display intermediaries have comprehensive advertising policies, which vary between companies, but they tend to cover the following areas:

● Ad creatives and landing pages

● Misleading claims, behaviours, and content

● Prohibited and restricted advertising categories

● Intellectual property protection

● Data collection

These policies generally incorporate the requirements of the CAP Code. Some go further on certain issues, such as restricting or prohibiting the advertising of contentious products (e.g. alcohol) or services (e.g. gambling); or restricting aspects of a category, or to whom it can be advertised. The following tables provide an indicative and selective summary of prohibitions and restrictions. Each advertising policy has specific details and different restrictions: for example, gambling ad restrictions may apply to online gambling only, not betting shops. Restrictions generally apply to age targeting (e.g. energy drinks on TikTok must be 18+ targeted; Google restricts the advertising of all food and drink to under-18s).

Table 12: Categories of product/service prohibited by platform policies, UK – selected examples

Category	TikTok[127]	Snap[128]	Twitter[129]	Google[130]	Meta[131]
Alcoholic drinks	X				
Cigarettes / e-cigarettes, vaping	X	X	X	X	X
Crypto currencies/ exchanges	X				
Debt consolidation	X		X		
Payday loans		X	X		X
Get rich quick	X	X			
Gambling	X				
Invasive cosmetic surgery	X		X		
Weight loss/management	X	X	X		

---

[127] https://ads.tiktok.com/help/article?aid=10005234 Accessed 23 April 2022

[128] https://www.snap.com/en-GB/ad-policies#financial-products Accessed 23 April 2022

[129] https://business.twitter.com/en/help/ads-policies.html#Ads Accessed 23 April 2022

[130] https://support.google.com/adspolicy/answer/6008942?visit_id=637853749644855889-1889855132&rd=1 Accessed 23 April 2022

[131] https://www.facebook.com/policies/ads/ Accessed 23 April 2022

Table 13: Categories of product/service restricted by platform policies, UK – selected examples

Category	TikTok[132]	Snap[133]	Twitter[134]	Google[135]	Meta[136]
Alcoholic drinks		X	X	X	X
Crypto currencies/ exchanges	X	X	X	X	X
Financial services	X	X	X	X	X
Gambling		X	X	X	X
Energy drinks	X			X	
HFSS food/drink	X			X	
OTC medicines	X	X			X

The smaller platforms (TikTok, Snap, Twitter) tend to apply more bans, whereas Google and Meta's policies lean more towards management through restrictions rather than outright prohibition. TikTok has the most rigorous stance towards prohibition of certain categories (e.g. alcohol and gambling).

The platforms' policies are regularly updated to keep pace with politics, laws and societal trends; for example:

- In 2022, platforms banned advertising by Russian state-owned entities[137].

- In July 2021, Meta introduced restrictions that prevent advertisers from targeting people under 18 on its platforms based on their interests or their activity on other sites[138].

- In August 2021, Twitter prohibited misleading 'before and after' photos, content that could be reasonably considered to body shame a customer, and promotion of unhealthy or unsafe eating behaviours or eating disorders. It also banned promoting dangerous supplements that look similar to prescription drugs or claim to increase the speed of weight loss and muscle growth[139].

---

[132] https://ads.tiktok.com/help/article?aid=10005234 Accessed 23 April 2022

[133] https://www.snap.com/en-GB/ad-policies#financial-products Accessed 23 April 2022

[134] https://business.twitter.com/en/help/ads-policies.html#Ads Accessed 23 April 2022

[135] https://support.google.com/adspolicy/answer/6008942?visit_id=637853749644855889-1889855132&rd=1 Accessed 23 April 2022

[136] https://www.facebook.com/policies/ads/ Accessed 23 April 2022

[137] Example - Snap Inc: https://www.snap.com/en-GB/ad-policies#prohibited-content

[138] https://www.reuters.com/technology/facebook-will-restrict-ad-targeting-under-18s-2021-07-27/

[139] https://business.twitter.com/en/help/ads-policies/ads-policy-update-log.html

Industry and self-regulatory initiatives

In 2020, a Plum Consulting report commissioned by the DCMS[140] identified a wide range of industry and self-regulatory initiatives that help to address the problems of harmful online advertising. Since then, there have been various developments in this area. The following are selected highlights. The scope of this project did not include conducting a comprehensive review of these initiatives.

- **Stop Scams UK**[141]. This organisation was formed in 2019, with members including Google, Microsoft, BT, Barclays, Lloyds Banking Group and HSBC. Meta joined in March 2022[142]. It is working to "stop scams at source", noting the prevalence of criminals posing as members of the banking, tech and telecoms sectors in order to scam their victims. The group is centred around technical collaboration and initiatives.

- **Scam Ad Alert System.** The ASA Scam Ad Alert System launched in 2020 in partnership with major online and social media platforms, including Google and Facebook. It receives reports from consumers (via a quick reporting form[143]) and passes these on to relevant platforms. Over the period June 2020 to September 2021 participating platforms and networks who responded to an ASA information request removed or suspended 765 ads and/or accounts as a direct result of information provided by the Scam Ad Alert System. 135 of these related to alerts for an ad seen on their platform and 630 to alerts for an ad seen on other platforms, highlighting the value of cross-platform intelligence sharing.

- **TAG TrustNet.** Following a 12-month trial, in October 2021 TAG announced the launch of TAG TrustNet in partnership with Fiducia[144]. This represents a Distributed Ledger Technology (DLT) initiative for the open display advertising market with the aim of building trust and transparency across the supply chain. In January 2022, Innovate UK, a UK government innovation agency, awarded a grant to TAG TrustNet to support the development of the initiative[145].

- **EDAA AdChoices.** The mission of the European Interactive Digital Advertising Alliance (EDAA) is to provide the AdChoices icon to companies active in digital advertising in Europe. This icon is displayed on digital ads and links through to its Consumer Choice Platform, usually via an interstitial page, enabling people to learn about data-driven advertising and exercise control over it. In some ad tech intermediary implementations (the interstitials differ between vendors), there is the possibility for consumers to report harmful advertising (e.g. Google). In Great Britain, awareness of the icon (with the 'Ad Choices' ad marker text) increased from 34% in 2016 to 50% in 2020, and the proportion of people who had clicked on the icon increased from 27% to 40%[146].

Current regulation and industry initiatives relating to body image

At present, the ASA may categorise advertising that has the potential to contribute to body image concerns as misleading, harmful or otherwise socially irresponsible, depending on the nature of the underlying issue[147]. CAP and BCAP Code rules on social responsibility[148] have been applied to uphold complaints

---

[140] Plum Consulting, Mapping online advertising issues, and the industry and regulatory initiatives aimed at addressing them, May 2020.

[141] https://stopscamsuk.org.uk

[142] https://www.standard.co.uk/news/uk/meta-facebook-hsbc-instagram-google-b988333.html

[143] https://www.asa.org.uk/make-a-complaint/report-an-online-scam-ad.html

[144] https://www.fiducia.eco/post/tag-launches-tag-trustnet-in-partnership-with-fiducia

[145] https://ipa.co.uk/news/tag-trustnet

[146] EDAA, European Advertising Consumer Research Report 2021.

[147] In such cases, the ASA's role is to weigh up, on the one hand, the advertiser's commercial freedom of expression and, on the other hand, restrictions that are necessary to protect the audience from misleading, harmful or offensive expressions. Where the ASA determines there is little likelihood of advertising causing harm, it cannot justifiably seek amendments to or withdrawal of such ads, no matter the strength of opinion articulated by the complainant. This balancing test is set by law; as a body exercising public functions, the ASA must observe this test.

[148] CAP Code rule 1.3 and BCAP Code 1.2): Marketing communications must be prepared with a sense of responsibility to consumers and to society.

against ads featuring models who appear overly thin (in an aspirational context, in some cases) and ads for cosmetic interventions which exploit individuals' insecurities about their bodies. The ASA can also investigate ads that use digital editing to alter body parts in images if it suspects the editing may result in a potential breach of the Code. In addition, the advertising Codes prohibit the targeting of weight reduction and cosmetic intervention ads at children through the selection of media or the context in which they appear [149],[150]. Body image is an area of self-regulatory development, with the potential for changes in the Codes. In 2021, the ASA launched a call for evidence to assist in their regulation of advertising which gives rise to potential harms relating to body image[151].

The advertising industry is also addressing the issue of body image. The Be Real campaign, founded by Dove and the YMCA, launched the Body Image Pledge[152] calling for the responsible portrayal of body image by the advertising, fashion, media and music industries. In April 2022, Ogilvy UK announced that it will no longer work with influencers who distort or retouch their bodies or faces[153]. Social media platforms have policies that prohibit or restrict some advertising that may contribute to body image concerns - in the UK:

● Meta's advertising policy on personal health[154]states: ad content must not imply or attempt to generate negative self-perception in order to promote diet, weight loss or other health-related products. Adverts for cosmetic procedures, weight loss products and services, and dietary, health or herbal supplements must be targeted to users aged over 18[155].

● Snap prohibits adverts for health and dietary supplements that promote weight loss, contain exaggerated or unrealistic claims, or include "before and after" pictures related to weight loss. The latter two prohibitions also apply to diet and fitness adverts. Adverts for plastic surgery must be targeted to people aged over 18[156].

● TikTok prohibits advertising of invasive cosmetic procedures and weight loss/management fasting products or services, including supplements[157]. It also prohibits ad content that depicts, promotes, normalises, or glorifies any dangerous weight loss behaviours associated with disordered eating[158]. It allows advertising of licensed cosmetic clinics provided that adverts target users aged over 18.

● Twitter prohibits the promotion of unacceptable business practices, including misleading 'before and after' text or images, use of content that could be reasonably considered to 'body-shame' the customer, and encouragement, glamorization, or promotion of unhealthy or unsafe eating behaviours or eating disorders[159]. It also prohibits knowingly advertising certain categories of products and services to minors, including weight loss, health and wellness supplements, ultraviolet tanning, and permanent cosmetics[160].

---

[149] CAP, Body Image in Advertising: Call for Evidence, 21 October 2021.
[150] https://www.asa.org.uk/news/strict-new-rules-for-ads-for-cosmetic-interventions.html
[151] https://www.asa.org.uk/resource/body-image-call-for-evidence.html
[152] https://www.berealcampaign.co.uk/resources/body-image-pledge
[153] https://www.thedrum.com/news/2022/04/07/ogilvy-will-no-longer-work-with-influencers-who-edit-their-bodies-or-faces-ads
[154] https://www.facebook.com/business/help/2489235377779939
[155] https://www.facebook.com/policies/ads
[156] https://snap.com/en-GB/ad-policies#disclosures
[157] https://ads.tiktok.com/help/article?aid=10005234
[158] https://www.tiktok.com/community-guidelines?lang=en
[159] https://business.twitter.com/en/help/ads-policies/ads-content-policies/unacceptable-business-practices.html
[160] https://business.twitter.com/en/help/ads-policies/ads-content-policies/prohibited-content-for-minors.html

International Regulatory Developments

The regulatory framework for online advertising differs by country and is highly complex. In most cases, these frameworks involve consumer protection, data protection, media, communications, and vertical market laws as well as self-regulatory codes, and are enforced by government agencies and self-regulatory bodies. This section does not describe these frameworks, but provides an overview of selected recent developments that affect the way that online advertising is regulated, focusing on the areas covered by the Online Advertising Programme in the UK, such as regulation of harms relating to online advertising content and targeting.

New European Union laws introduce rules and obligations for major online advertising platforms in the areas of transparency, behavioural targeting and privacy. Developments within certain European countries address specific issues such as responsible influencer marketing and use of retouched images in advertising. In the US, the Federal Trade Commission (FTC) is addressing certain online advertising issues and there are legislative proposals relating to privacy. These developments complement existing self-regulatory systems in these countries.

European Union

The main recent developments in advertising regulation at the European Union level are the proposed Digital Services Act and the Digital Markets Act which will regulate major digital platforms and certain other companies that intermediate between businesses and consumers. Rules and obligations around online advertising form part of these Acts.

Digital Services Act

The proposed Digital Services Act (DSA) regulates the obligations of digital services that act as intermediaries in their role of connecting consumers with goods, services and content. It is intended to protect consumers and fundamental rights online, create a transparency and accountability framework, and fairer and more open digital markets[161]. Rules will be harmonised across the EU and cover areas including illegal content, traceability of business users in online marketplaces, safeguards for users, transparency, obligations for very large platforms to prevent abuse of their systems, and researcher access to data. Enforcement of the DSA will be through national and EU-level cooperation. Each Member State will appoint a Digital Services Coordinator responsible for supervising intermediary services established in their Member State. It will have the power to impose penalties specified in national law in line with the Regulation.

The DSA applies to online intermediaries, which includes services such as internet service providers, cloud services, messaging, marketplaces and social networks. Specific obligations apply to online platforms, such as social networks, content-sharing platforms, app stores, online marketplaces, online travel and accommodation platforms. A subset of rules specified in the DSA apply to very large platforms, which have a significant societal and economic impact , reaching at least 45 million users in the EU, representing 10% of the population[162].

On 20th January 2022, the European Parliament voted to approve the text of the DSA, including a range of amendments[163]. Political agreement was then reached on 23 April 2022[164], though the final text of this agreement was not available at the time of writing. As of the January 2022 amendments, the DSA requires online platforms to empower consumers around targeting practices, be more transparent, prohibit targeting of minors and vulnerable groups, and provide access to data and algorithms. Intermediaries in the open

---

[161] https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348
[162] https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348
[163] https://www.theregister.com/2022/01/22/eu_dsa_draft_meps/
[164] https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2545

display ecosystem would be covered by voluntary codes of conduct around transparency. The main rules around advertising include[165]:

- **Prohibition of "dark patterns".** Users should be able to make free and informed choices about advertising practices, and intermediary services shall not use practices (e.g. "dark patterns") to exploit cognitive biases to prompt users to reveal information they do not want to. (Amendment 40, Recital 39a).

- **Easy withdrawal of consent.** Online platforms should ensure that users can refuse or withdraw consent for targeting advertising, in accordance with the GDPR, in a way that is not more difficult nor time-consuming than to give their consent. Refusing consent in processing personal data for the purposes of advertising should not result in access to the functionalities of the platform being disabled. Alternative access options should be fair and reasonable both for regular and for one-time users, such as options based on tracking-free advertising. (Recital 52, Amendments 57 and 498).

- **Online platforms transparency.** Online platforms should provide users with information about when and on whose behalf an advert is displayed, including who finances the advert. They should also provide people with easy access to information about the main parameters used for determining that specific advertising is displayed to them, providing meaningful explanations of the logic, including when this is based on profiling. (Recital 52, Amendments 57 and 498).

- **Codes of conduct for intermediary transparency.** The Commission shall encourage and facilitate the drawing up of voluntary codes of conduct at Union level between, online platforms and other relevant service providers, such as providers of online advertising intermediary services or organisations representing recipients of the service and civil society organisations or relevant authorities to contribute to further transparency for all actors in the online advertising ecosystem. The effectiveness of the codes should be regularly assessed. In order to enhance accountability, participation and transparency, procedural safeguards for drawing up codes of conduct are needed. (Article 36, Amendment 372; Recital 70, Amendment 74).

- **Prohibition of targeting of minors.** Online platforms should not use personal data for commercial purposes related to direct marketing, profiling and behaviourally targeted advertising of minors. The online platform should not be obliged to maintain, acquire or process additional information in order to assess the age of the recipient of the service. (Recital 52, Amendments 57 and 498).

- **Prohibition of targeting of vulnerable groups based on special category data.** Targeting individuals on the basis of special categories of data which allow for targeting vulnerable groups should not be permitted. (Recital 52, Amendments 57 and 498).

- **Provision of ad libraries.** Very large online platforms should ensure public access to repositories of adverts displayed on their online interfaces to facilitate supervision and research into emerging risks. Repositories should include the content of adverts, including the name of the product, service or brand and the object of the advert, and related data on the advertiser, and, if different, the natural or legal person who paid for the advert, and the delivery of the advert, in particular where targeted advertising is concerned (including the audiences the advertiser wishes to reach). In addition, very large online platforms should label any known deep fake videos, audio or other files. The repository should hold adverts until one year after the last time the advert was displayed, and be searchable through easy to access, efficient and reliable tools. (Recital 63, Amendment 68; Article 30, Amendment 332).

---

[165] Amendments adopted by the European Parliament on 20 January 2022 on the proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (COM(2020)0825 – C9-0418/2020 – 2020/0361(COD))

- **Access to data and algorithms.** The Digital Services Coordinator or the Commission may require access to or report of data and algorithms to assess the risks and harms of a very large platform's advertising systems. The Regulation provides a framework for compelling access to data from very large online platforms to vetted researchers, not-for-profit bodies, organisations or associations. All requirements for access to data under that framework should be proportionate and appropriately protect the rights and legitimate interests, including personal data, trade secrets and other confidential information, of the platform and any other parties concerned, including the recipients of the service. Vetted researchers, not-for-profit bodies, organisations or associations should guarantee the confidentiality, security and integrity of the information, such as trade secrets, that they obtain when performing their tasks. (Recital 64, Amendment 69).

The DSA also introduces a notice and takedown regime for illegal content that includes a range of obligations. Examples include measures for notice and action, an obligation to provide information to users, and trusted flaggers. These measures may apply to illegal online advertising content.

Digital Markets Act

The proposed Digital Markets Act (DMA) introduces rules for platforms that act as gatekeepers in the digital sector, with the aim of preventing these platforms from imposing unfair conditions on businesses and consumers and ensuring openness of digital services. The DMA will apply to companies that provide a core platform service (search, social networking, messaging, operating systems, online intermediation) in at least three Member States, have an annual turnover in the European Economic Area of €6.5 billion or more (or a market capitalization of at least €65 billion); control an important gateway for business users towards final consumers (more than 45 million monthly active end users in the EU and more than 10,000 yearly active business users established in the EU); and an (expected) entrenched and durable position[166].

Gatekeepers will be required to interoperate with third parties in specific situations, allow business users to trade outside gatekeeper's platforms, and provide business users with access to the data generated by their activities on the gatekeeper's platform. Gatekeepers will also be prevented from blocking users from uninstalling pre-installed software or apps, using data obtained from their business users to compete with these business users, and restricting users from accessing services acquired outside of the gatekeeper platform. The DMA will be enforced by the European Commission. Penalties for non-compliance with the DMA include fines of up to 10% of the company's total worldwide annual turnover and periodic penalty payments of up to 5% of the company's total worldwide daily turnover.

The DMA includes specific transparency rules relating to online advertising. According to the amendments adopted by the European Parliament on 15th December 2021[167], gatekeepers must:

- **Provide pricing transparency information relating to the programmatic supply chain.** Gatekeepers are required to 'provide advertisers and publishers to whom they supply online advertising services, with free of charge, effective, high-quality, continuous and real-time when requested and to the extent possible, with information that allows both sides to understand the price paid for each of the different advertising services provided as part of the relevant advertising value chain and the availability and visibility of advertisement'. (Recital 42, Amendment 29) The Act specifies categories of information including bids placed by advertisers and intermediaries, price-setting mechanisms and calculation of fees, price and fees paid by the advertiser and publisher, and the amount and remuneration paid to the publisher. (Article 5, Amendments 111 to 116) This measure is intended to tackle opacity in the programmatic advertising value chain, but is likely to apply only to Google, Meta and Amazon, given the definition of gatekeepers. Other intermediaries in the open display advertising supply chain would not be covered.

---

[166] https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2349

[167] Amendments adopted by the European Parliament on 15 December 2021 on the proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) (COM(2020)0842 – C9-0419/2020 – 2020/0374(COD))

- **Use business users' advertising data only for the provision of the advertising service.** Gatekeepers who play a dual role of intermediary (between businesses and end users) and as providers of advertising services (to allow businesses to advertise to end users), are prohibited from using advertising data of business users to compete with them. They are also prohibited from 'disclosing any commercially sensitive information obtained in connection with one of its advertising services to any third party belonging to the same undertaking and from using such commercially sensitive information for any purposes other than the provision of the specific advertising service unless this is necessary for carrying out a business transaction'. (Recital 44, Amendment 30).

- **Provide access to performance measurement tools and information to allow independent verification.** Gatekeepers need to provide the companies advertising on their platform with access to the performance measuring tools of the gatekeeper and the information necessary for advertisers and publishers to carry out their own independent verification of their advertisements hosted by the gatekeeper. They should provide 'advertisers and publishers for entire disclosure and transparency of the parameters and data used for decision making, execution and measurement of the intermediation services. A gatekeeper should further provide when requested, with free of charge access to the performance measuring tools of the gatekeeper and the information necessary for advertisers, advertising agencies acting on behalf of a company placing advertising, as well as for publishers to carry out their own independent verification of the provision of the relevant online advertising services.' (Recital 53, Amendment 36).

- **Refrain from personalised targeting without clear, informed consent.** A gatekeeper shall 'for its own commercial purposes, and the placement of third-party advertising in its own services, refrain from combining personal data for the purpose of delivering targeted or micro-targeted advertising, except if a clear, explicit, renewed, informed consent has been given to the gatekeeper in line with the procedure laid down in the Regulation (EU) 2016/679 by an end-user that is not a minor.' (Article 6, Amendment 120).

The text of the DMA was provisionally agreed by European Parliament, European Council and European Commission negotiators on 24th March 2022[168]. The final text was not available at the time of writing.

---

[168] https://www.europarl.europa.eu/news/en/press-room/20220315IPR25504/deal-on-digital-markets-act-ensuring-fair-competition-and-more-choice-for-users

Other European regulation

Several other areas of European regulatory development are also relevant to online advertising:

- The **ePrivacy Regulation** is a proposed law to replace the existing ePrivacy Directive (Directive 2002/58/EC). The European Council approved a position on the Directive on 10 February 2021[169], since when the Directive has been in trilogue negotiations. Of relevance to advertising, the Directive aims to streamline consent requests for cookies by enabling the use of browser settings to accept or refuse tracking cookies and other identifiers[170]. However, text mandating browsers to provide the option to prevent data collection and force users to select their privacy preferences during installation has been removed[171].

- The **Memorandum of Understanding (MoU) on Intellectual Property Rights (IPR)** was facilitated by the European Commission and the first version was signed in June 2018[172]. The signatories of this MoU commit to minimise the placement of advertising on websites and mobile applications that infringe copyright or disseminate counterfeit goods[173].

- The **Unfair Commercial Practices Directive** dates to 2005 and was intended to boost consumer confidence and make it easier for businesses, especially small and medium-sized enterprises, to trade across borders. On 17 December 2021, the European Commission adopted a new Commission Notice on the interpretation and application of the Directive, providing new guidance[174]. With respect to online advertising, this guidance clarifies that:

    - Social media platforms can present an increased risk of "hidden advertising" (e.g. native advertising that blends content and commercial communications) and that all forms of commercial communications (advertising) should be disclosed, (Section 4.2.5).

    - Influencer marketing (including paid posts, affiliate content, retweets or tagging the trader/brand) must make clear that a trader has paid for the promotion of the product and that this should be prominent. This also applies if the influencer is endorsing its own products or business. (Section 4.2.6).

    - Personalised persuasion practices based on linking data from different sources, continuous testing to learn more about consumer behaviour (e.g. A/B testing), and without the full knowledge of the consumer may be manipulative and unfair under consumer law. It adds that these practices may have a more significant effect on vulnerable consumers, and that the concept of vulnerability is dynamic and situational (someone can be vulnerable in one situation but not in others). The use of information about the vulnerabilities of specific consumers or a group of consumers for commercial purposes could amount to a form of manipulation in which the trader exercises undue influence over the consumer and is prohibited. The guidance highlights that direct exhortations to children are prohibited. (Section 4.2.7).

---

[169] https://www.euractiv.com/section/digital/news/mixed-emotions-as-council-finally-adopts-position-on-eprivacy-text/
[170] https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation
[171] https://iabeurope.eu/proposed-eprivacy-regulation/
[172] https://iabeurope.eu/european-digital-policy/#pp-toc-6095231194fdc-anchor-2
[173] https://ec.europa.eu/growth/industry/strategy/intellectual-property/enforcement-intellectual-property-rights/memorandum-understanding-online-advertising-and-ipr_en
[174] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021XC1229%2805%29

European country-level developments

Certain EU Member States and other European countries have introduced legislation or self-regulatory initiatives that address online advertising harms. The following list provides selected examples. This project did not involve conducting a thorough review of developments country-by-country.

- In Norway, the 2009 Marketing Act has been amended[175] to make it **illegal for influencers to share retouched photos of their body in promotional posts** on social media, without acknowledging the image has been edited[176]. The government will provide guidance on how retouched images should be labelled. This legislative change was made in response to concerns around body image in influencer marketing.

- In France, ARPP[177], the self-regulatory body for advertising, set up a monitoring scheme that used artificial intelligence and humans to review over 30,000 content items across over 7,000 influencers for compliance with identification requirements[178]. It has also launched a **Responsible Influencer Certificate** to encourage influencer awareness and compliance[179].

- In Germany, the **Network Enforcement Law**[180] (Netzdurchsetzunggesetz or NetzDG) came into force in 2017. It places obligations on social networks with more than two million users in Germany to handle complaints about unlawful content and to publish a biannual transparency report. The law refers to 21 criminal statutes under the Germany Criminal Code (StGB), which fall into the broad categories of hate speech or political extremism, terrorist or unconstitutional content, violence, harmful or dangerous acts, defamation or insult, privacy, and sexual content. Social networks must take down obviously unlawful content within 24 hours of a complaint and, where legality is not obvious, 7 days. Transparency reports must include data about the number of complaints, the number of complaints that resulted in take down, and take down times, among other information. NetDG refers to content and does not specifically mention advertising, though at a minimum social media influencer paid promotions would fall under the definition of content. The limited list of criminal statutes in scope restrict NetzDG to tackling only extreme forms of harm in this advertising. According to H2 2021 NetzDG transparency reports, the most complained about categories of content on YouTube[181] were hate speech or political extremism, defamation or insults, and sexual content, while on Facebook[182] the main issues were defamation, insult and incitement to hatred.

- In Ireland, the Member State in which Meta, Google and Twitter are established in the European Union, the **Online Safety and Media Regulation Bill**[183] was published in January 2022. It establishes the Media Commission, a new regulatory body, and creates a regulatory framework including a definition of harmful online content, and binding online safety codes.

---

[175] https://www.stortinget.no/no/Saker-og-publikasjoner/Vedtak/Beslutninger/Lovvedtak/2020-2021/vedtak-202021-146/

[176] https://i--d-vice-com.cdn.ampproject.org/c/s/i-d.vice.com/amp/en_uk/article/88nmy4/norway-retouching-social-media-law

[177] Autorité de Régulation Professionnelle de la Publicité

[178] https://www.arpp.org/actualite/resultats-observatoire-influence-responsable-2021/

[179] https://www.arpp.org/certificat-influence-responsable-inscriptions/

[180] https://germanlawarchive.iuscomp.org/?p=1245

[181] https://transparencyreport.google.com/netzdg/youtube?hl=en

[182] Facebook, NetzDG Transparency Report, January 2022

[183] https://www.gov.ie/en/publication/d8e4c-online-safety-and-media-regulation-bill/

United States

In the US, advertising is regulated by federal and state law, with the Federal Trade Commission (FTC) taking a leading role, alongside self regulation. Advertisers are the main subject of this regulation. Relevant federal laws include the FTC Act, the Lanham Act and the Dodd-Frank Wall Street Reform and Consumer Protection Act. States also regulate advertising through consumer protection statutes and statutes regulating certain practices. The FTC is the main regulator responsible for enforcing federal laws relating to advertising, while state attorneys general and local district attorneys enforce state and local laws. Certain vertical market agencies also have a role in regulating advertising in their industries, such as US Food and Drug Administration (FDA) which regulates drug advertising. There are also various self-regulatory bodies, such as the National Advertising Division (NAD)[184].

The FTC is applying existing law to address some emerging online advertising issues, backed up by the threat of strong penalties. For example, in November 2021 it provided guidance about the disclosure of advertising in social media influencer posts[185]. The FTC has the power to issue substantial fines. In March 2020, it reached a settlement requiring Teami, a maker of detox teas, to return $1 million to consumers due to misleading claims and influencers not disclosing paid endorsements about the products which continued after an initial warning in 2018[186]. It also sent letters to the influencers concerned warning that influencers who fail to make adequate disclosures about their connections to marketers are subject to legal enforcement action by the FTC[187]. In October, 2021, the FTC sent a Notice of Penalty Offenses to more than 700 businesses about influencer marketing and a range of other practices relating to endorsements, testimonials and reviews that it considers to be deceptive[188]. This forms a basis for potential future action in these cases.

In the privacy field, the FTC has also fined OpenX, an online open display advertising intermediary, $2 million for allegations of collecting personal information from children under 13 without parental consent, a violation of the Children's Online Privacy Protection Act Rule (COPPA Rule)[189]. Democratic lawmakers introduced the Banning Surveillance Advertising Act (BSAA) which would prohibit advertisers from targeting ads to consumers, with certain exceptions[190].

---

[184] Frankfurt Kurnit Klein & Selz PC, Advertising and marketing in the USA, 11 April 2019.

[185] https://www.ftc.gov/system/files/documents/plain-language/1001a-influencer-guide-508_1.pdf

[186] https://www.ftc.gov/news-events/news/press-releases/2020/03/tea-marketer-misled-consumers-didnt-adequately-disclose-payments-well-known-influencers-ftc-alleges

[187] https://www.ftc.gov/system/files/documents/cases/1823174teamiwarningletters.pdf

[188] https://www.fenwick.com/insights/publications/ftc-issues-notice-of-penalty-offenses-for-endorsement-and-testimonial-marketing

[189] https://www.ftc.gov/news-events/news/press-releases/2021/12/advertising-platform-openx-will-pay-2-million-collecting-personal-information-children-violation

[190] https://www.adexchanger.com/privacy/even-if-targeted-online-advertising-isnt-banned-take-note-of-which-way-the-wind-is-blowing/

Annex 1: Review of Online Advertising Harms

The following sections provide an update on the nature and scale of consumer and industry harms relating to online advertising, as set out in the taxonomy of harms. Where possible, the study team has illustrated each category of harm with real examples drawn from the media, industry reports, use of services, and a review of the Meta Ad Library. Importantly:

- Meta is the only platform to offer a comprehensive searchable ad library[191]. **The use of examples of harmful advertising on Facebook or Instagram in this document does not imply that other social media platforms do not also serve harmful advertising** - though these other platforms are currently less transparent than Meta.

- Ad Library operates a keyword search. Searches were conducted on selected keywords related to relevant harms. Bad actors (i.e. criminals) are likely to avoid using ad wording that references any activity in violation of platform policies. Therefore, many instances of harmful advertising may have gone unidentified by these searches.

- The Ad Library shows only ads that are currently running[192]. Therefore, it does not provide information about ads that were identified as harmful and taken down by Meta. Some of the examples presented in this document may have subsequently been taken down by Meta or have stopped running, thus they will no longer be available to view in the Library.

Each section provides an indicative rating of the relative incidence and severity of the category of harm using the following key. These ratings are based on the assessment made in section 2.2.

Relative incidence/severity: 🟡 = Low, 🟠 = Medium, 🔴 = High.

Trend: ⇩ = Decreasing, ⇨ = Relatively stable, ⇧ = Increasing.

Malicious advertising

Relative **incidence**: 🔴 High | Relative **severity**: 🔴 High | **Trend**: ⇨ stable

Malicious advertising (also referred to as malvertising) is specific to open display advertising and involves the use of malicious computer code. This code is delivered via the advertising creative content (the electronic file that represents the ad) or an ad tag or landing page. It executes on the user's browser and/or device to steal information, take over the browser or device, or download unwanted content. In many cases, the intention is to perpetrate fraud, such as using hijacked browsers to generate false actions that fuel attribution fraud (a form of ad fraud) or using stolen data or passwords to access people's financial services. As such, there is an overlap between this category of harm and fraudulent advertising, below.

The level of malicious advertising is relatively low as a proportion of total ad impressions, but high in absolute terms due to the large number of impressions served every day. Cyber security vendor Confiant estimates that about 0.159% of programmatic open display ad impressions had a security violation in Q4 2021, including malicious clickbait, forced redirects, criminal scams and other dangerous activity[193]. This number excludes malicious ads that go undetected. This is likely to account for around a million or more open display advertising impressions daily, given that billions of impressions are served daily in the UK.

Levels of malicious advertising are elevated in the alternative display advertising ecosystem (see Supply chains section). Cyber security company White Bullet found that fraud and malware represented 3% of UK ad impressions on piracy apps and 19% of ads on piracy websites[194].

It is difficult to determine the impact of malicious advertising. Where malicious advertising initiates fraud, such as the theft of data in order to hack bank accounts, individual losses can be significant. However,

---

[191] Snap Inc. has a political ad library.
[192] With the exception of ads that are about issues, elections or politics where Meta stores ads in the library for 7 years.
[193] Confiant, Malvertising and Ad Quality Index , Q4 2021
[194] White Bullet, How regulation and outreach reduce ad placement on piracy websites, 2022.

consumers hacked in this way are unlikely to know that malicious advertising led to malware attacks that led to these losses.

Example: Hidden malicious ads

This mobile ad hides behind a legitimate-looking ad and mimics an error message in appearance. The user is tricked into pressing 'install' which downloads malware onto the device, allowing cyber criminals to hijack the user or deliver a payload (malicious software)[195].

Figure 17: Example of a hidden malicious mobile ad
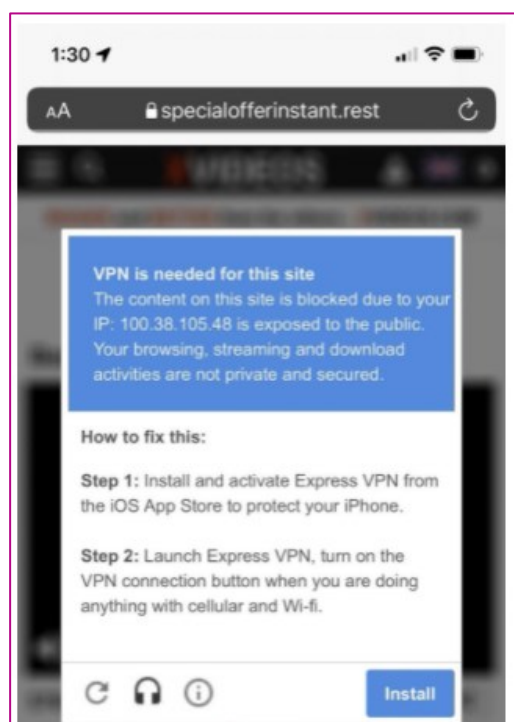
Fraudulent advertising, including scams

Relative **incidence**: ● High | Relative **severity**: ● High | **Trend**: ⇧ Increasing

Paid-for online advertising is used to promote a range of frauds and scams. Since 2020, there appears to have been an increase in the variety of scams, with recent reports including but not limited to:

- **Celebrity clickbait-driven cryptocurrency/financial scams.** These scams generally involve ads linking to fake news articles about rapid profit from cryptocurrency investing (and in some cases binary trading and foreign exchange), with links to scam websites designed to defraud victims. Ads may appear on paid search, open display or social display. In open display ads, scammers generally use cloaking methods to spoof landing pages (deceive intermediaries and platforms into believing that the landing page is a legitimate website the scammer has mimicked). They also operate a large number of domains (websites).

- **Clone scams (diversion fraud).** Scammers buy sponsored search advertising for keywords relating to trusted brands. The ads display URLs similar to the trusted brand URL and click through to "clone" websites designed to look identical to trusted brand websites. Consumers are defrauded through phishing (capturing personal information and passwords for e.g. banking services) on fake website logins or by telephone on fake customer services numbers provided on the clone sites[196]. In shopping

---

[195] https://www.confiant.com/news/bad-mobile-ads-contribute-to-churn

[196] https://www.theguardian.com/money/2021/jul/15/retired-detective-lost-life-savings-in-a-clone-firm-investment-scam

clone scams (see below), consumers are scammed into paying for non-existent products. In clone cryptocurrency wallet scams, fraudsters buy search terms referring to popular crypto wallets, such as Phantom and MetaMask. These ads direct consumers to imitations of these crypto wallets where phishing scams are perpetrated[197].

- **Government services copycats and intermediaries.** Copycat websites offer government services such as driving licence and passport renewals with little to no additional benefit. In 2018, five people were convicted for defrauding UK consumers with websites that mimicked government agency sites[198]. In 2021, Which? found that "rip off" intermediary sites were using Google and Bing to advertise expensive driving licence renewal services that consumers don't need, in violation of platform policies[199]. Results for Google and Bing searches on 'driving licence renew' both put 3 sponsored listings for 'rip off' intermediary sites ahead of the DVLA website listing[200].

- **Investment scams.** According to the Financial Conduct Authority (FCA), investment and trading scams usually involve promises of guaranteed high returns. A search on the term '50% return on investment' on Facebook Ad Library yielded results including an ad for InveXup labelled '50% minimum guaranteed ROI' which appears to be too good to be true (see below). Google and Bing searches for the same term returned no suspicious paid-for results.

- **Miracle health scams.** Advertising promises that products such as creams or cannabidiol (CBD) items cure chronic or terminal diseases, provide rapid weight loss or offer other implausible health benefits. Ads often click-through to fake news pages supporting their claims, with onward links to ecommerce sites. These ads appear on paid search (see below). The project team did not find examples on Facebook Ad Library.

- **Online shopping fraud.** Consumers are enticed by products advertised at heavily discounted rates, then find that after paying, these products are not delivered or are substituted by lower-value products. Commonly, the retailer website disappears shortly afterwards in a classic exit scam. Which? reported ads for these frauds appearing on social media and sponsored search results[201].

- **Subscription scams.** This is a variant of online shopping fraud where a consumer buys an item(s) at an online checkout, then later discovers they have been signed up to a monthly payment subscription without their knowledge.

- **Fake ticketing/ticket fraud.** Websites offer consumers tickets to events, often when the tickets are either not yet available or are sold out. After purchasing, consumers either never receive tickets, or receive fake tickets that will not gain them entry into the event when checked by security. The websites used to do this often have similar URLs to well known and trusted legitimate ticket selling websites.[202] It is unclear the extent to which these websites are advertised with paid-for advertising.

- **Other cryptocurrency scams.** Various schemes, such as ads luring consumers with cryptocurrency giveaways: a search of Facebook Ad Library using the term 'Bitcoin giveaway' identified results for 7 active and inactive ads[203], including an ad that advertises Elon Musk 'Giving out Bitcoin'[204]. These ads have the hallmarks of scams, but have not been validated as such.

---

[197] https://www.theverge.com/2021/11/4/22763015/cryptocurrency-fake-wallet-phishing-scam-google-ads-phantom-metamask

[198] https://www.asa.org.uk/news/asa-welcomes-sentencing-of-criminals-behind-fraudulent-copycat-websites.html

[199] https://www.which.co.uk/news/2021/06/rip-off-checking-firms-appear-in-73-of-driving-licence-renewal-searches-which-warns/

[200] Searches conducted by Spark Ninety on 21 March 2022.

[201] https://www.which.co.uk/news/2020/11/nearly-one-in-ten-scammed-by-adverts-on-social-media-or-search-engines/

[202] https://www.actionfraud.police.uk/a-z-of-fraud/ticket-scams

[203] Search conducted on 23/02/2022

[204] Facebook ad ID 267529162030891 appeared on Instagram, Facebook and Messenger.

- **Other frauds.** Fraud involving promotion by online advertising reported to Action Fraud in 2020/21 included the categories of betting, competitions, courses, employment offers, fake legal documents, rentals and pets (buying of puppies and kittens)[205] - in addition to the categories listed above.

In many cases, scams involve fake celebrity endorsement on the ad and/or a scam website (see next section). Ads for these scams may appear on open display, social display, sponsored search, and less frequently on social media influencer posts. The mix of these channels used varies by category of fraud. For example, clone scams use search advertising in order to narrowly target search terms related to the cloned brand.

Table 23: Relative levels of scam advertising by category of paid-for advertising - indicative guide

Category	Open display	Social display	Search	Influencer
Celebrity clickbait driven scams	●●●	●●○	●●○	○○○
Clone scams (diversion fraud)	○○○	●○○	●●●	○○○
Copycat government site scams	○○○	●○○	●●●	○○○
Investment scams	●○○	●●○	●●●	●○○
Miracle health scams	●○○	●●○	●●●	●○○
Online shopping scams	●○○	●●○	●●○	○○○
Subscription scams	○○○	●●○	○○○	○○○

Key: ○○○ = low, ●●● = high. Comparison of levels is valid within rows not between rows.

There are high levels of scam advertising in the UK, especially celebrity clickbait driven scams:

- From 1 March 2021 to 25 March 2022 the ASA received 1,251 reports of potential scams via its quick reporting form (Scam Ad Alert system) of which 23% (288) were in scope (fitted the definition of a scam, involved paid-for advertising) and 6% (67) resulted in Scam Ad Alerts. The majority of the scams for which the ASA issued alerts fit the description of celebrity clickbait scam advertising. Of the scam ad alerts 14 (21%) related to ads seen on social media sites and 53 (79%) related to ads seen in other online media, such as open display advertising on publisher websites or apps.

- Over the period June 2020 to September 2021 participating platforms and networks who responded to an ASA information request removed or suspended 765 ads and/or accounts as a direct result of information provided by the Scam Ad Alert System. 135 of these related to alerts for an ad seen on their platform and 630 to alerts for an ad seen on other platforms, highlighting the value of cross-platform intelligence sharing.

- 35,115 Action Fraud reports in 2020/21 were identified as being related to fraud enabled by online advertisements, based on keyword analysis. Total estimated loss from these reports was about £400 million[206]. This data includes fraud initiated by paid-for advertising and non-paid for advertising such as organic search results and social media posts. Only fraud reports where victims self-reported relevant keywords (e.g. ads, pop up, banner) are counted, therefore this data is likely to underestimate the total number of reported frauds initiated by online advertising.

---

[205] City of London Police / National Fraud Intelligence Bureau, Fraud Enabled by Online Adverts 2020/21 – Dip Sample report, November 2021. Involved analysis of Action Fraud reports. Quoted in the DCMS consultation on reviewing the regulatory framework for online advertising in the UK: The Online Advertising Programme - Impact Assessment.
[206] City of London Police / National Fraud Intelligence Bureau, Fraud Enabled by Online Adverts 2020/21 – Dip Sample report, November 2021. Involved analysis of Action Fraud reports. Quoted in the DCMS consultation on reviewing the regulatory framework for online advertising in the UK: The Online Advertising Programme - Impact Assessment.

- An estimated 9 million people (17%) have been targeted by a scam on social media, according to a nationally representative survey conducted by Which? in November 2021[207]. This data includes paid-for advertising as well as other forms of targeting on social media.

- An estimated 300,000 people in the UK were victims of subscription frauds, with total losses of approximately £75m, according to fraud investigator Gillian Schonrock[208]. These estimates do not distinguish between fraud initiated by paid-for advertising and organic (non paid-for) social media posts.

The frequency of scam advertising and losses from it are likely to have increased since 2020, though data is limited and does not capture the period after platforms introduced financial services advertiser verification in 2021.

- The Media Trust, a digital safety company, found that the number of distinct outbreaks of malicious programmatic display scam ads it detected increased 66% from 1,213 in December 2020 to 2,013 in May 2021[209]. Scam ad attacks generally occur in spikes.

- Investment fraud losses in the UK almost doubled from £55.2 million in the first half of 2020 to £107.7 million in the same period in 2021[210]. UK Finance claim that many of those who fall victim to such scams do so after seeing enticing adverts on social media[211].

- In the US there is rapid growth in all forms of fraud originating on social media, though the data does not distinguish between fraud originating from paid-for advertising, organic non-paid for advertising, and messaging on social media platforms.

Figure 18: US reports of and losses from fraud originating on social media[212]
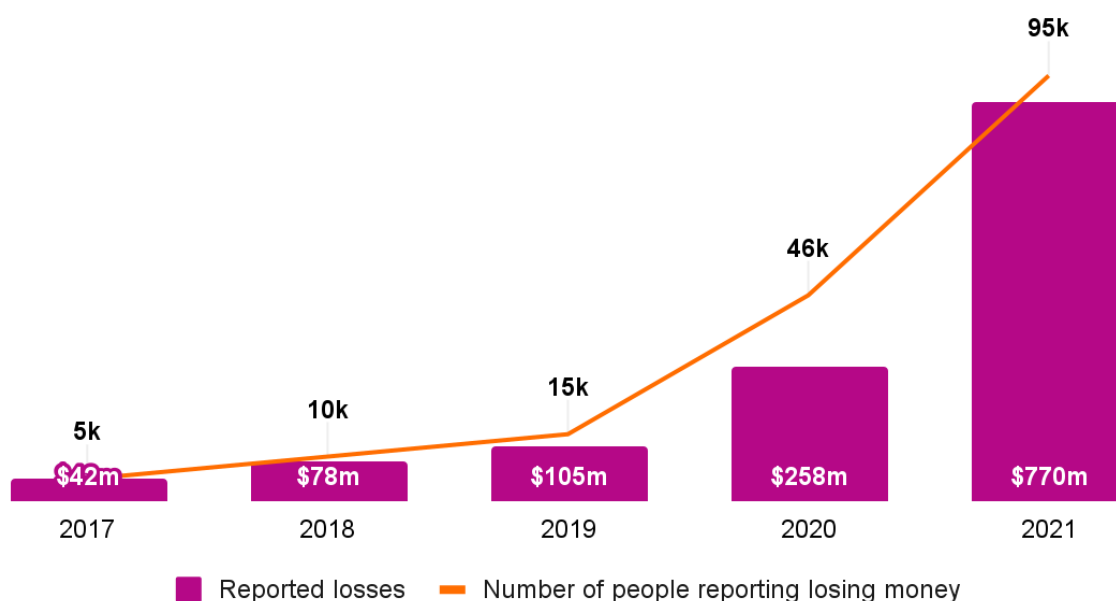
Figure based on fraud reports directly to the FTC indicating a monetary loss and identifying social media as the method of contact.

---

[207] https://press.which.co.uk/whichpressreleases/paid-for-advertising-desperately-needed-in-the-online-safety-bill-amid-epidemic-of-fraud-which-warns/

[208] Quoted by BBC, https://www.bbc.co.uk/news/uk-60464668

[209] The Media Trust, Scam Ads: Evolution and increase in Scam ads in the Digital Ecosystem, June 2021.

[210] UK Finance, 2021 Half Year Fraud Report, 22nd September 2021.

[211] https://www.ukfinance.org.uk/press/press-releases/government-coordinated-action-needed-fraud-losses-rise-30-cent

[212] FTC, Data Spotlight, Social media a gold mine for scammers in 2021, January 2022.

Although the overall level of scam advertising is high, there appears to have been a reduction in the amount of investment scam advertising in paid search results, following the introduction of UK financial services advertiser verification[213] on 30 August 2021. Which? conducted a Bing search for 'compare best savings rates' on 20th September 2021, revealing adverts for 4 firms listed by the FCA as potentially harmful[214]. A Spark Ninety repeat of this search on Google and Bing on 20th March 2022 yielded no adverts for companies on the FCA's warning list, indicating a potential improvement.

Example - Celebrity clickbait cryptocurrency scams

The following example shows a celebrity clickbait cryptocurrency scam found from a sponsored search result[215]. ① Sponsored Google search result for the term "investment schemes". ② Fake news article with the false celebrity endorsement (in this case the use of Holly Willoughby and Philip Schofield appearing to discuss the matter on television). ③ Cryptocurrency scam page that unwitting users are then taken to by the link in the fake article.

Figure 19: Scam advert, landing page and scam page

---

[213] https://support.google.com/adspolicy/answer/10770884?hl=en-GB
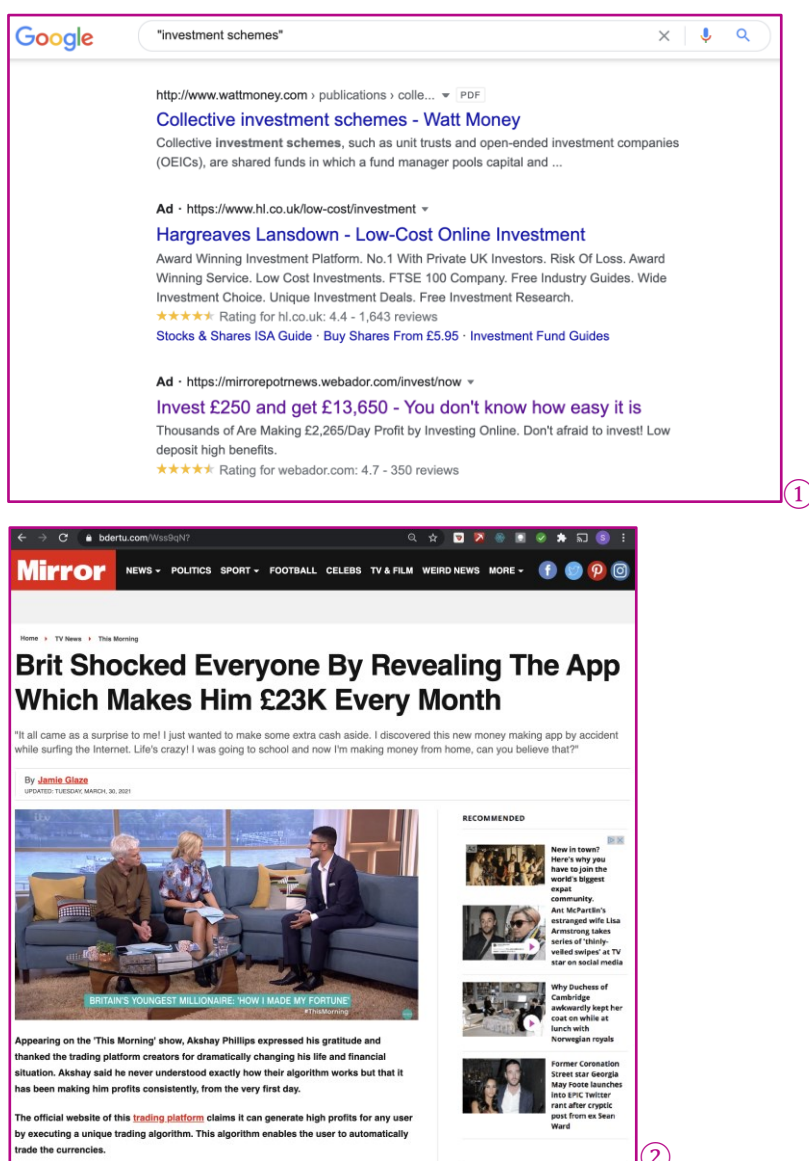
[214] https://www.which.co.uk/news/2021/10/fake-ads-rife-on-bing-as-investment-scams-jump-84/.

[215] Google search conducted on 30th March 2021. Google has since introduced verification of financial services advertisers to address financial scam ads.
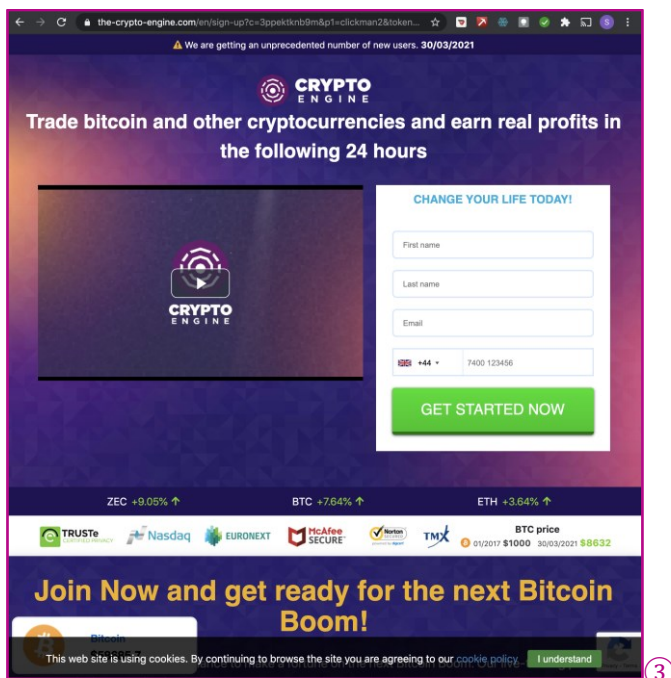
③

Example: Clone scams - Search advertising for clone sites

The following example shows a clone scam for the bank Revolut. ① Sponsored Google search result for the term "Revolut Business" which is placed by a clone website. ② Clone website where people are defrauded.

**Figure 20: Search result and landing page (website) for a clone scam**
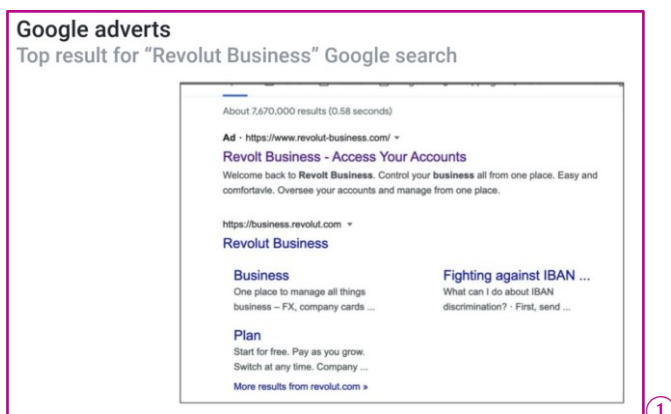
①
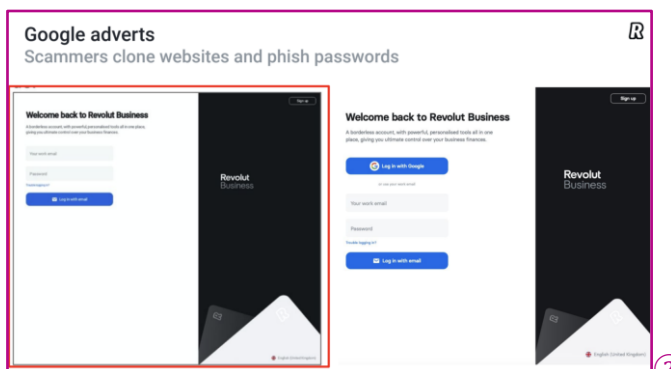
②

Example: Search advertising placed by sites intermediating government services[216]

The following example illustrates search results for the term "driving licence renew" on ① Google and ② Bing. In each case, three sponsored results from "rip off" intermediary sites are listed ahead of the DVLA website. These sites are not fraudulent, but the DVLA advises people to use the official government website when applying for driving licence renewals[217].

Figure 21: Search results for 'driving licence renew'
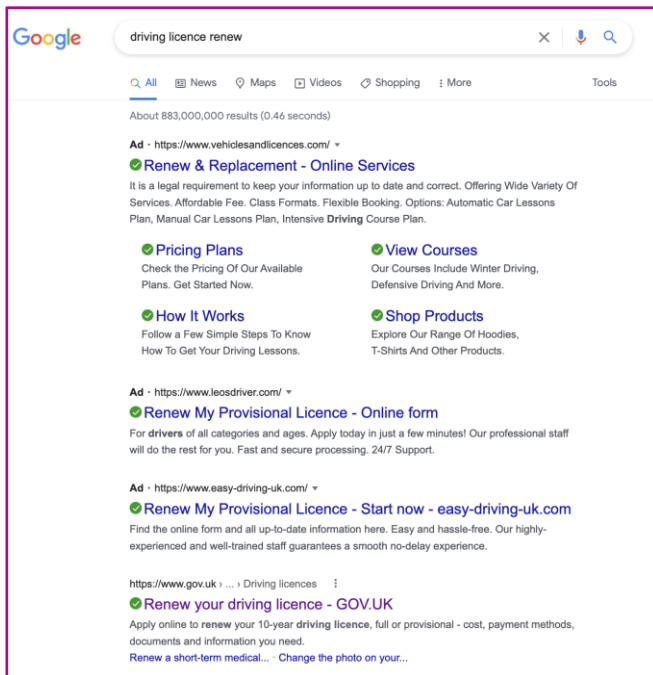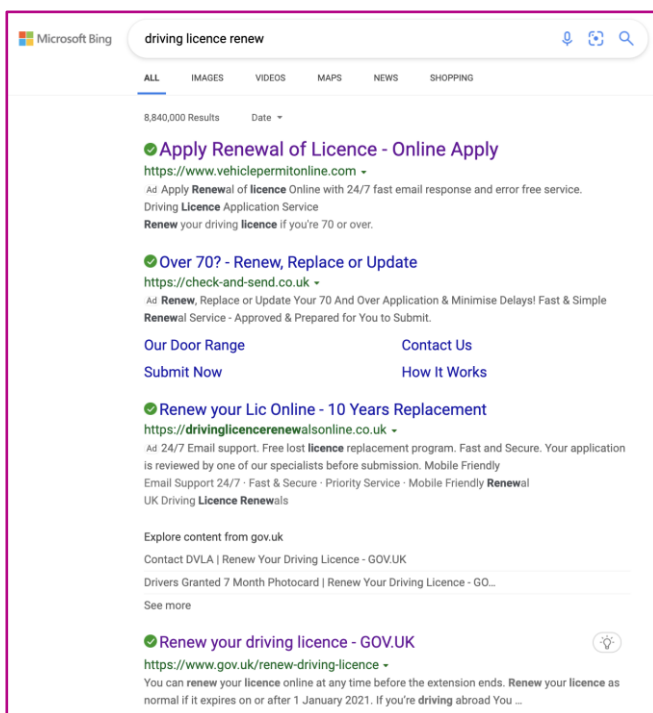
Example: Health scams - weight loss creams and pills advertised on paid search[218]

The following examples show Bing search results for ① "weight loss cream"[219] and ② "lose weight permanently pills"[220]. The sponsored search results are likely to include "miracle health" scam products, though it was not possible to test these products as part of this project.

Figure 22: Search results for 'weight loss cream' and 'lose weight permanently pills'
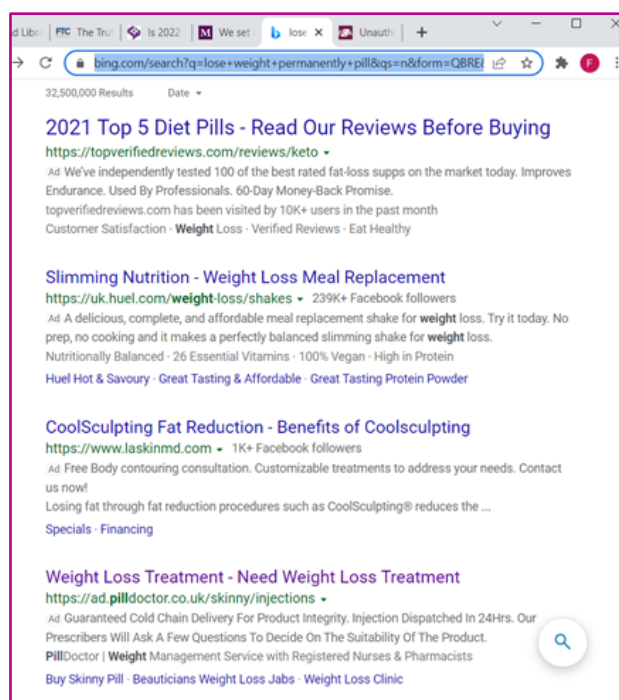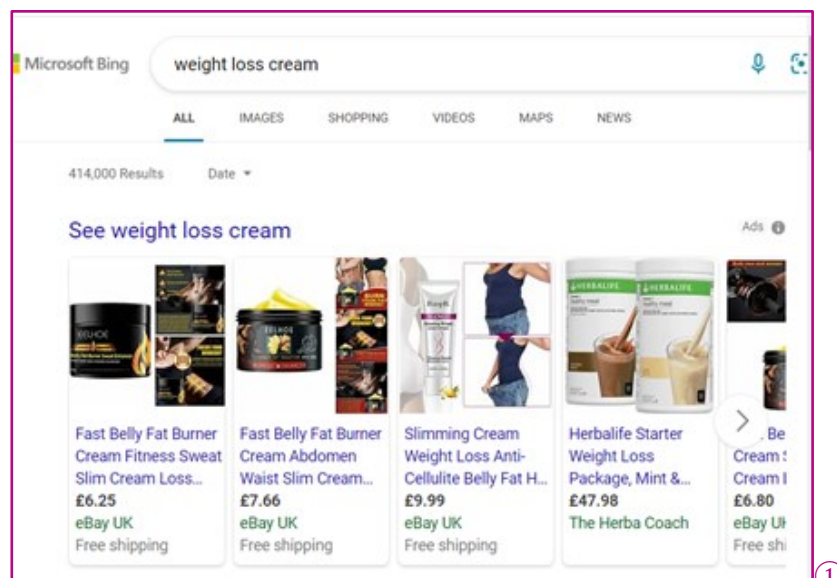
Figure 23: Example: Possible investment scam - InveXup Facebook ad promising 50% ROI per annum[221]

It was not feasible as part of this project to test whether this advert is for a scam, but there are reasons for suspicion: the advertised return on investment appears too good to be true and InveXup is not on the FCA Financial Services Register.

Unsanctioned use of celebrity images

In many cases, scams use fake celebrity endorsement to lend credibility to their claims or otherwise use celebrity images as a form of clickbait. Generally, scammers fake endorsement from celebrities who are known for their business or financial acumen or are otherwise well known and trusted. Recent examples of fake endorsement include:

- Duke and Duchess of Sussex - Bitcoin-related investment scams[222]

- Gareth Southgate - Bitcoin Bank cryptocurrency scam[223]

- Martin Lewis - Binary trading, energy companies, PPI reclaim firms, mortgage brokers and more[224]

- Peter Jones - CBD gummies and 'miracle health' products for conditions, e.g. arthritis

- Deborah Meaden - Health supplements[225]

- Holly Willoughby - Investment scams[226]

- Sir Richard Branson - Investment scams[227]

---

[221] Facebook ad ID 1065404874316160, started running on Facebook and Messenger on 17 February 2022. Ad Library searched on 3 March 2022.
[222] https://www.bbc.com/news/uk-60040937
[223] https://www.thetimes.co.uk/article/gareth-southgate-seeking-legal-advice-after-name-used-in-crypto-scam-fzgw75rbd
[224] https://www.moneysavingexpert.com/shopping/fake-martin-lewis-ads/
[225] https://conversation.which.co.uk/scams/dragons-den-fake-cbd-oil-deborah-meaden/
[226] https://www.thesun.co.uk/tech/12276183/fake-celebrity-endorsements-online-ads-scam/
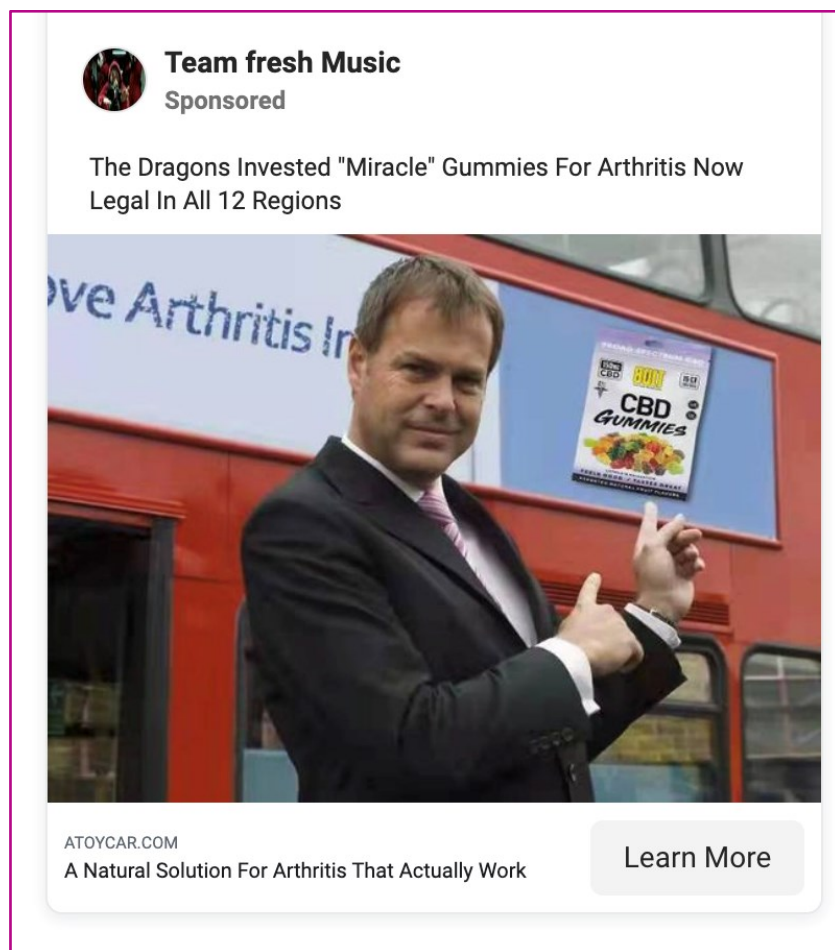[227] https://www.ncsc.gov.uk/news/celebrity-scam-tackled-by-ncsc

- Jeremy Clarkson - Bitcoin-related investment scams[228]

Celebrity images are generally shown in ad creative copy and on landing pages. In some cases, celebrity images are incorporated into faked compositions, such as the celebrity pointing at a product or brand image. To date, fake endorsement has been limited to static display ads in the social and open display markets. It is likely that video and audio celebrity likenesses and endorsements would be more difficult to fake. However, criminals might develop the capability to create fake celebrity videos in the near future. In 2021, a Russian ad agency licensed the rights to Bruce Willis's likeness and used artificial intelligence to create a deep fake video representation of him[229].

Although there is limited data about the scale of fake celebrity endorsement, media reports about the issue appear to be increasing in frequency and encompass a growing range of personalities. In November 2021, 14 celebrities wrote to the Prime Minister to demand action on this issue[230].

Fake endorsement can amplify consumer harms caused by scams (see above) and cause reputational damage to celebrities. Scammers may be able to evade platform and intermediary ad checks by avoiding direct reference to celebrity names, using fuzzy or side-angle celebrity images, and running multiple ad versions from multiple accounts to avoid take-down after detection.

Figure 24: Peter Jones's image used to advertise 'CBD gummies' as a cure for arthritis[231]

---

[228] https://www.thisismoney.co.uk/money/beatthescammers/article-7508643/Beware-Bitcoin-Revolution-scam-fake-Clarkson-endorsement.html
[229] The Drum, Lessons from the agency that deepfaked Bruce Willis for a Russian ad campaign, September 2021.
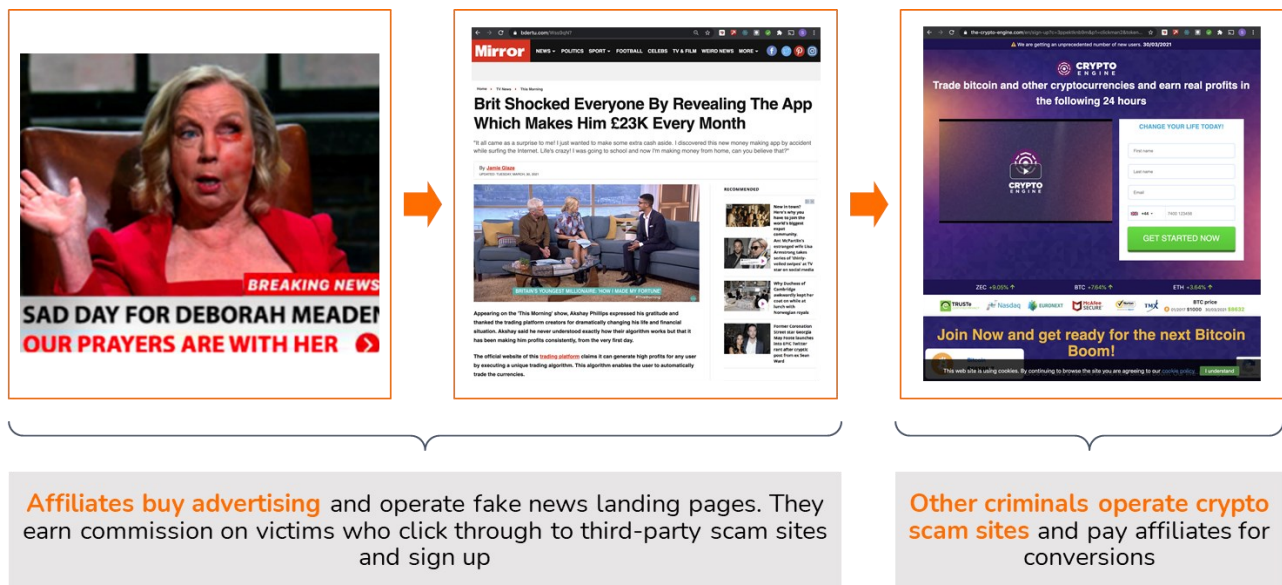[230] https://www.moneysavingexpert.com/news/2021/11/martin-lewis--sir-richard-branson--deborah-meaden-plus-11-other-/
[231] Ad ID 4942916352422521 started running on 16/02/2022 across Facebook, Messenger, Instagram. Identified in Facebook Ad Library on 22/02/2022.

Anatomy of a scam

Cyber security sources indicate that celebrity clickbait scam advertising is generally perpetrated by cyber criminals operating as "affiliates". Their role is to place ads that drive visitors to cryptocurrency scam websites operated by other criminal organisations. Affiliates earn a commission of about $600 for each visitor who "converts" (invests in the scam), according to an investigation conducted in the Netherlands, with operators of scam websites making an average of $3,000 per victim[232]. It is likely that these criminal affiliates advertise via social media, search and email, as well as online open display advertising, given that similar ads linking to similar fake news/cryptocurrency scam landing pages have been detected on these media.

Figure 13: The main criminal participants involved in celebrity clickbait scam advertising

Affiliates buy advertising and operate fake news landing pages. They earn commission on victims who click through to third-party scam sites and sign up

Other criminals operate crypto scam sites and pay affiliates for conversions

Cyber criminal affiliates generally buy advertising through companies they set up to look like advertising agencies. They buy advertising using multiple DSPs to limit the impact if a DSP account is blocked. In some cases, criminals use "cloaking" techniques to evade DSP advertising quality reviews. This technique involves creating reputable looking ads and landing pages, in some cases mimicking known brands, to show to ad scanners (tools used by DSPs to check ads for malware or other policy infringements). These ads exist in parallel with malicious ads and landing pages. In one operating model, the advertiser ad server is programmed to serve ad scanners with innocuous reputable looking ads and landing pages, while serving malicious advertising to targeted victims. The techniques used to evade detection are constantly evolving.

There are a range of contributory factors that enable cyber criminals to run scam advertising campaigns, limit the effectiveness of efforts to detect and take down these campaigns, and limit the deterrent effect.

---

[232] https://www.npo3.nl/brandpuntplus/de-verborgen-industrie-die-bitcoinadvertenties-op-facebook-zet-ze-weten-niet-eens-dat-we-bestaan

Table 14: Factors contributing to the problem of celebrity clickbait scam advertising

Factors enabling scam attacks to occur	Factors limiting detection and mitigation of attacks	Factors limiting the threat of penalties
• Criminal actors can access the ecosystem due to limited due diligence on advertisers/agencies • Screening of ad creative and landing pages is limited and misses some scam ads	• Consumer reporting and complaints systems are fragmented and complex • There is no consistent identification of advertisers/agencies throughout the programmatic ecosystem • Some intermediaries are slow to respond to reports of scam advertising and block ads	• Cyber criminals operate from overseas jurisdictions and are difficult for UK law enforcement to reach • There is limited law enforcement resource to tackle scam advertising

Counterfeiting

Relative **incidence**: 🟠 Medium | Relative **severity**: 🟠 Medium | **Trend**: ⇨ stable

Ecommerce is one of the top 3 ways that UK consumers buy counterfeits, including major ecommerce sites or "rogue" or "scam" websites[233]. Counterfeiting is focused on high-margin branded product categories, such as fashion, beauty, toys and electricals. Like legitimate ecommerce, counterfeit products and services are often promoted by paid-for advertising.

Counterfeiting is relatively widespread, but there is limited data about the extent of paid-for online advertising of counterfeits:

- 29% of UK consumers had knowingly purchased counterfeits and 16% had done so unknowingly[234]. The proportion of these consumers who purchased counterfeits online is unknown.

- 9% of EU consumers have been duped into buying counterfeit goods by online advertising[235], but the extent of paid-for advertising vs. organic (non paid-for) advertising is unknown. Industry reports imply that organic search and social media promotion are the primary issues.

- Paid-for social influencer marketing of counterfeits appears to be a large problem and is likely to be growing. 10% of UK female consumers were prompted by social media endorsements to buy counterfeits, and 13% of female UK consumers are more likely to purchase a counterfeit that is promoted by an influencer[236]. Major influencers such as the Kardashians and Jenners have promoted counterfeits.

- More than 70 consumer and apparel companies were confirmed to have been targeted by fraudulent and infringing sponsored adverts on Instagram and Facebook from May 2017 to July 2020[237].

- Google removed 1.2 million ads for counterfeit goods globally in 2020. A further 46 million ads were removed for copyright infringements, and 200 million for trademarks[238].

---

[233] Intellectual Property Office, Counterfeit goods research, 2 September 2020
[234] Intellectual Property Office, Counterfeit goods research, 2 September 2020
[235] European Union Intellectual Property Office, European Citizens and Intellectual Property report, 2020
[236] Intellectual Property Office, Influencer report, November 2021
[237] Transnational Alliance to Combat Illicit Trade (TRACIT), Fraudulent Advertising Online: Emerging Risks and Consumer Fraud, 2020.
[238] Google, Ads Safety Report, 2020.

There are recent examples of paid-for counterfeit advertising across search, social display and classifieds, and influencer marketing. Anecdotally, there appears to be a shift from advertising on paid search to social media due to stronger ad safety procedures on Google Ads (buying platform of Google search ads).

Counterfeiting costs brands £9bn per annum in the UK in lost revenue, and accounts for 80,500 job losses annually[239]. There is no data about the proportion of this loss that stems from paid-for online advertising of counterfeits. The proceeds of counterfeiting may fund terrorist groups, or organised crime groups that are linked to human trafficking[240].

Consumers who unknowingly purchase counterfeits are harmed by not receiving the product they expected. In certain cases, consumers are also harmed by counterfeit products that do not meet safety standards: 32% of UK consumers who had purchased more than one counterfeit good had suffered a health issue as a direct result, according to a 2018 report[241]. A social influencer was left with chemical burns after applying counterfeit make up[242].

Major platforms have recently strengthened their policies and tools to deal with counterfeits. Meta provides brands with a Commerce and Ads IP Tool that enables businesses to upload images of their brand and products for matching against Facebook and Instagram content in order to detect counterfeit listings[243]. One of the main reasons for paid-for advertising of counterfeits appears to be a lack of stringent checks on advertisers and ad creative and landing pages. The influencer marketing ecosystem is more open to counterfeit ads through bilateral deals between influencers (often small scale) and advertisers, without checks on advertisers taking place.

Example: Kendall and Kylie Jenner promotion of fake AirPods

Kendall and Kylie Jenner (members of the Kardashian family) advertised knock-off Apple AirPods on Instagram posts they made in 2020. At the time, they had a combined following of 322 million Instagram accounts (this has subsequently increased to 526 million as of 11th February 2022). Although Apple had previously pursued sellers of products infringing its intellectual property, it reportedly pursued neither Kylie nor Kendall.

Figure 25: Illustration of an Instagram story from Kendall Jenner advertising fake Apple AirPods[244]

---
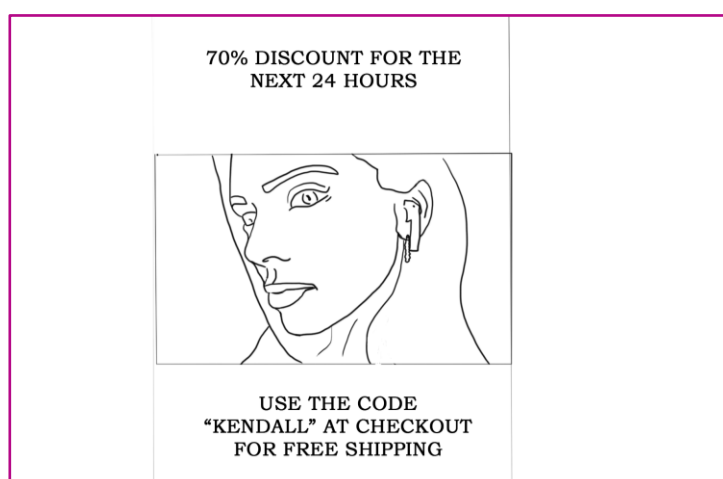
[239] Intellectual Property Office, Counterfeit Goods Research, 2 September 2020.

[240] European Police Office, Serious and Organised Crime Threat Assessment, 2013.

[241] https://www.incoproip.com/reports/counterfeit-products-are-destroying-brand-value/

[242] https://www.itv.com/news/2017-12-06/fake-makeup-the-toxic-truth-you-need-to-know-this-christmas

[243] https://www.socialmediatoday.com/news/facebook-adds-new-tools-to-enable-content-creators-and-ip-holders-to-detect/597214/

[244] Image of the Instagram story available at: BBC, https://www.bbc.com/news/technology-53596192

Example: Facebook ad for fake Versace clothing

A Facebook ad from 'Luxury Outfit', launched on 2nd March 2022, advertises knock-off Versace clothing[245]. Whilst it is not advertised as 'replica' or 'fake', it can be assumed that the products on the linked website are fake, as they include misspellings of the brand name, and are sold at suspiciously low prices.

Illegal and restricted activities, products and services

Relative **incidence**: 🟠 Medium | Relative **severity**: 🔴 High | **Trend**: ⇨ stable

Online advertising is being used to promote products, services or activities that are illegal or restricted in the UK - and to promote legal products where advertising is illegal or restricted. Paid-for advertising of the most seriously harmful categories of illegal products, such as firearms and category A drugs, appears to be rare. However, there is a problem with organised crime groups (OCGs) advertising sexual services provided by trafficked people under their control. These adverts are placed primarily on classified advertising platforms, including some generalist classifieds platforms and specialist classifieds platforms that focus on adult services, known as Adult Service Websites (ASWs). The adverts placed by OCGs generally mimic legitimate adverts placed by self-determined sex workers and may be paid-for advertising or free listings.

The scale of this problem is likely to be large, but is challenging to estimate due to the hidden nature of modern slavery and human trafficking. The demand for sexual services in the UK is high. The UK market leading ASW received approximately 1.26 million visits per month from December 2020 to May 2021. The number of potential victims of modern slavery referred to the Home Office increased by 20% in the last year; from 10,601 victims in 2020 to 12,727 in 2021. Sexual exploitation accounted for 16% of referrals in 2021[246] (over 2,000 people). When the police rescue victims of sexual trafficking, in the overwhelming majority of cases they are advertised on ASWs[247].

There are several factors contributing to OCGs being able to place adverts on ASWs. First, it is difficult to distinguish adverts placed by OCGs from adverts placed by self-determined sex workers. ASWs may need to investigate advertiser IP addresses and credit card details to identify links between adverts, for example. Second, age verification and moderation processes are inconsistent across different ASWs.

There is also online advertising that promotes legal products and services where advertising is prohibited in law, such as:

- Tobacco products[248]. In 2021, 26 UK influencers with a combined following of 2.2 million Instagram users advertised nicotine products from the company Velo.

- Prescription drugs or unlicensed drugs. Some influencers have been promoting the unlicensed weight gain drug Apetamin[249]; its status as an unlicensed drug means it has not passed the required regulatory tests to ensure its safety, and thus it should not be sold, supplied or advertised[250].

- Unregistered clinics offering cosmetic procedures, such as lip fillers. Some influencers have been found to promote a competition requiring them to follow accounts run by Play Social, that in turn promoted services ranging from unregistered lip filler injection clinics to breast enhancement surgery[251].

In addition, some advertising closely relates to illegal products, but is not prohibited (see the 'Legal but harmful' section, below). Facebook was found to carry advertising for weapons-related products (e.g. body

---

[245] Facebook ad ID 3130939743830652, launched 02/03/2022 on Facebook

[246] Modern Slavery: National Referral Mechanism and Duty to Notify statistics UK, end of year summary, 2021.

[247] National Crime Agency, Briefing: Adult Service Websites, April 2022.

[248] The Tobacco Products Directive that came into effect in the UK in 2016 prohibits advertising for nicotine-containing e-cigarettes not licensed as medicines on on-demand television, in newspapers and magazines, on the internet, in emails and in text messages

[249] https://news.sky.com/story/apetamin-nhs-urges-instagram-to-clamp-down-on-dangerous-weight-gain-drug-12293940

[250] https://www.bbc.com/news/health-56930654

[251] https://www.independent.co.uk/life-style/instagram-influencers-plastic-surgery-gambling-b1856973.html

armour, tactical gear) that do not fall under the definition of weapons[252]. It responded by introducing a ban of weapons-associated gear[253].

Platform and intermediary policies generally prohibit illegal advertising. In July 2021, Google announced a clamp down on advertising of weapons, drugs and other illegal products. It introduced a 3 strike system whereby advertisers would be banned from Google platforms if they were found to be violating the terms of service regarding illegal products 3 times[254].

Google removed 12.9 million ads for 'dangerous products/services' globally in 2020[255], though it is unclear how this category is defined and whether these ads were stopped before they started running or after some consumers had been exposed to them.

Example: Influencer promotion of prescription drugs

In April 2020, influencer Gemma Collins took to Instagram to post a paid-for Story advertising 'SkinnyJab', a weight-loss injection that contained prescription-only medicine[256]. Whilst the product is not illegal, prescription-only medicines may not be advertised to the public. The ASA banned the advertising.

Figure 26: Illustration of a Gemma Collins post advertising SkinnyJab

[252] https://www.theguardian.com/commentisfree/2021/jan/26/facebook-ads-combat-gear-rightwing-users

[253] https://www.reuters.com/business/media-telecom/facebook-ban-ads-promoting-weapon-accessories-protective-gear-us-2021-01-16/

[254] https://investorsking.com/2021/07/28/google-to-introduce-strike-based-system-to-clamp-down-on-advertisers-violating-google-ads-policies/

[255] Google, Ads Safety Report, 2020.

[256] Case: https://www.asa.org.uk/rulings/skinnyjab-ltd-a20-1064725-skinnyjab-ltd.html, Image of post available at: https://www.thesun.co.uk/tvandshowbiz/12865135/gemma-collins-breach-ad-rules-weight-loss-jab-posts/

Non-identified advertising

Relative **incidence**: 🔴 High | Relative **severity**: 🟡 Low | **Trend**: ⇧ Increasing

All advertising content must be obviously identifiable as such, and must be actively disclosed as advertising in scenarios where it is unclear to the audience that they are being advertised to. The ASA has a series of public rulings and public guidance, drawing out lessons from those rulings, that sets out what effective disclosure should look like. Children are likely to be especially susceptible to non-identified or subtly identified advertising. Ofcom found that just under half of 8–15-year-olds can correctly identify Google search ads, and two-thirds of 12-15s are aware that influencers might be sponsored by brands[257].

Recent issues with non-disclosure of advertising mainly relate to influencer marketing. In a limited 2020 study focused on influencers who had previously been contacted regarding non-disclosure of advertising, the ASA found that only 35% of subsequent Instagram posts from 122 influencers included the appropriate disclosures[258]. There is no available data for compliance levels among other influencers, though case reports indicate that there may be a high level of non-disclosure of advertising.

- An ASA ruling from February 2021 upheld a complaint against TikTok influencer Luke Mabbott. Within a sponsored collaboration with Boohoo.co.uk, his tag of #boohooman was deemed insufficient in clearly labelling the post as paid-for marketing[259].

- An ASA ruling from December 2021 upheld a complaint against Instagram influencer Adam Cuthbertson, after his Instagram story promoting a product from The Lowcal Ltd was not obviously identifiable as a marketing communication[260].

Influencers with large followings appear to have professionalised and are mainly compliant, with the main problems being unclear identification and non-identification among influencers with small followings. Ofcom qualitative research with 20 creators found that medium scale (5,000 to 15,000 Instagram followers) and large scale (20,000 or more followers) creators were typically aware of the need to declare advertising, but only some smaller scale creators (fewer than 5,000 followers) were aware[261]. However, there was confusion around the rules over what constitutes an ad.

This is supported by data from France where a study of content posted by over 7,000 influencers found that 73.4% posts were identified as advertising, of which 32.2% could be more clearly or immediately identified. Non-identification was a particular problem with small-scale influencers: 12.6% of influencers with more than 1 million followers failed to identify sponsored posts, while this figure rose to 43.1% for influencers with fewer than 10,000 followers[262].

Non-disclosure of influencer advertising is a global challenge. US influencers are widely followed by UK consumers, accounting for a quarter of the 20 most liked influencers in the UK[263]. The FTC has guidelines to help US influencers comply with the law around disclosure of paid promotions[264]. According to a Mediakix study conducted in 2017, 93% of the top Instagram influencers did not label their sponsored posts in accordance with the FTC regulations[265]. More recent data is not available.

In the US, the Strategic Organizing Center, a coalition of unions, raised a complaint with the Federal Trade Commission claiming that Amazon could be "unlawfully deceiving" customers because it doesn't clearly

---

[257] Ofcom, Children and parents: media use and attitudes report, 2020/21

[258] https://www.asa.org.uk/static/dd740667-6fe0-4fa7-80de3e4598417912/Influencer-Monitoring-Report-March2021.pdf

[259] https://www.asa.org.uk/rulings/boohoo-com-uk-ltd-in-association-with-luke-mabbott.html

[260] https://www.asa.org.uk/rulings/the-lowcal-ltd-g21-1121210-the-lowcal-ltd.html

[261] Ofcom, VSP Content Creators and Community Standards, September/October 2021.

[262] https://www.arpp.org/actualite/resultats-observatoire-influence-responsable-2021/

[263] YouGov, The most popular influencers in the UK, Q4 2021.

[264] FTC, Disclosures 101 for Social Media Influencers

[265] https://mediakix.com/blog/celebrity-social-media-endorsements-violate-ftc-instagram/

label sponsored search results[266]. According to the complaint, labels indicating that a search result is sponsored appear several seconds after a page loads, thus obfuscating ads for a short period. Sponsored search results on amazon.co.uk appear with the label 'sponsored' which was not noticeably delayed when tested in March 2022[267], indicating that this issue is not replicated in the UK and/or has been resolved.

Failure to disclose advertising can be harmful to users as it can give a false impression on the effectiveness of the services or products being advertised, as well as by not pushing users to think more critically about what they are seeing.

Example: Non-identified ads on Instagram

A post from Instagram influencer Amber Rose Gill promoted a beautician on 23rd December 2021, with no disclosure as to the nature of the arrangement of the promotion. The caption and demonstration video within the post heavily imply that it was a sponsored piece of influencer marketing, but the Instagram 'paid partnership' tool has not been used, and the caption does not feature identifying hashtags, such as '#ad' or '#sponsored'[268].

Figure 27: Illustration of an Amber Rose Gill social media post

Similarly, a post from Instagram influencer Chloe Khan on February 5th 2022 promoted a car rental service with a photograph and a caption, but with no disclosure as to the nature of the sponsorship arrangement[269]. Whilst we cannot categorically determine that these posts were paid-for sponsorships, the tagging of the

---

[266] https://www.washingtonpost.com/technology/2021/12/08/amazon-search-results-ftc-complaint/

[267] Various search terms were input into www.amazon.co.uk viewed on the Chrome desktop browser over a fibre broadband connection on 3 March 2022.

[268] https://www.instagram.com/p/CX1D0UXskNm/

[269] https://www.instagram.com/p/CZm8vlfMnzE/

relevant brands and the lengthy advocation of the brands, which are otherwise unrelated to the lives and work of the influencers involved, heavily suggests a paid arrangement.

Figure 28: Illustration of a Chloe Khan social media post

Misleading advertising

Relative **incidence**: 🔴 High | Relative **severity**: 🟠 Medium | **Trend**: ⇧ Increasing

Online advertising may mislead consumers by making false claims, failing to disclose risks, not substantiating claims, exaggerating, and a range of other reasons. 82% of ASA complaint cases about paid-for online advertising in 2021 related to potentially misleading advertising. The total number of these complaint cases increased by 51% to a total of 6,364 in 2021, driven by a 92% increase in potentially misleading social influencer advertising complaint cases to 3,541 in 2021. 27% of video sharing platform users say they were exposed to potentially harmful or misleading advertising, of whom 51% claimed to see this advertising at least weekly, and 53% took action such as clicking the report button[270]. 18% of users experienced harmful or misleading advertising on Facebook, 10% on Instagram, 9% on Twitter and 8% on YouTube. This data does not distinguish between misleading and other forms of harmful advertising, or paid-for and non-paid-for advertising; therefore, exposure to paid-for misleading advertising is likely to be below the 27% of video sharing platform users cited above.

---

[270] Ofcom, User Experience of Potential Online Harms within Video Sharing Platforms. Data is from the Ofcom Video-sharing platform usage & experience of harms survey 2021.

There are case reports of misleading ads across all online advertising categories: search, social display, open display, influencer marketing and classifieds. Issues that have emerged since 2020 include:

- Omission of risk warnings in ads for cryptocurrency investments. The ASA has upheld cases against social display ads for Skrill[271] and Coinbase[272], a YouTube influencer ad for Exmo[273], and an open display ad for eToro[274].

- Use of filters on images in influencer posts to mislead consumers about the effectiveness of cosmetic products. The ASA upheld a case against an influencer ad for a We are Luxe t/a Tanologist Tan product[275].

- Ads linked to misinformation. The ASA upheld a case against Pheka Agency Co Ltd for an ad claiming to offer protection from harm that it implied is caused by electromagnetic radiation produced by mobile phones and laptops[276].

One of the reasons for misleading online advertising is the large volume of advertising campaigns run by small-scale advertisers who are unlikely to invest as much attention to compliance as major brands.

Example: Use of filters on images in social influencer posts

A complaint against an ad from Instagram influencer Elly Norris for a tanning product from Skinny Tan was upheld by the ASA. It was deemed misleading for her use of an Instagram filter when demonstrating the effects of the product.[277]

Figure 29: Illustration of Elly Norris social influencer posts

---

[271] https://www.asa.org.uk/rulings/skrill-ltd-a21-1118717-skrill-ltd.html

[272] https://www.asa.org.uk/rulings/coinbase-europe-ltd-a21-1123058-coinbase-europe-ltd.html

[273] https://www.asa.org.uk/rulings/exmo-exchange-ltd-a21-1122405-exmo-exchange-ltd.html

[274] https://www.asa.org.uk/rulings/etoro--uk--ltd-a21-1123324-etoro--uk--ltd.html

[275] https://www.asa.org.uk/rulings/we-are-luxe-ltd-t-a-tanologist-tan-in-association-with-cinzia-baylis-zullo.html

[276] https://www.asa.org.uk/rulings/pheka-agency-co-ltd-a20-1064871-pheka-agency-co-ltd--unconfirmed-.html

[277] Elly Norris ASA case: https://www.asa.org.uk/rulings/skinny-tan-ltd-in-association-with-elly-norris.html

Example: Misleading debt clearance advertising

One common form of misleading ad is those that appear to advertise debt clearance services. The ad below ran across Facebook, Instagram and Messenger from 13th September 2021. In the view of the study team, it is similar to ads that the ASA has ruled against, upholding complaints against them for misleading consumers by overstating the ease with which debt can be cleared, falsely implying a relationship with a government department, and falsely implying that the advertiser is a debt clearance service themselves, rather than a company that hands leads onto third parties[278].

Figure 30: Social media advert for debt clearance

Offensive advertising

Relative **incidence**: 🟠 Medium | Relative **severity**: 🟡 Low | **Trend**: ⇧ Increasing

Although the CAP Code makes reasonable allowances for ads in bad taste and accepts that many adverts are likely to cause degrees of offence to some, it prohibits ads that are likely to cause serious or widespread offence to many people. The ASA notes that an ad shouldn't necessarily be banned just because some people find it awkward, unpleasant or irritating. Ads that are deemed to go beyond irritation and cause serious or widespread offence include ads containing violence, adult content, gore or otherwise shocking material, or causing offence on the grounds of race, religion, gender, sexual orientation, disability or age. When considering cases of offence, the ASA takes into account who is likely to see the ad, the context in which it appears (primarily what it is promoting), and the prevailing societal standards of the time[279].

6% of ASA paid-for online advertising complaint cases in 2021 related to offensive advertising. The total number of these complaint cases was 454, a 37% year-on-year increase. Video-on-demand services accounted for the largest proportion of complaint cases (35%), followed by social media (28%), web display (11%) and app display (10%).

---

[278] Facebook ad:
https://www.facebook.com/ads/library/?active_status=all&ad_type=all&country=GB&q=539253880675053&sort_data[direction]=desc&sort_data[mode]=relevancy_monthly_grouped&search_type=keyword_unordered&media_type=all
Related ASA article: https://www.asa.org.uk/news/asa-takes-action-against-misleading-debt-advice-ads.html
[279] Advertising Standards Authority, Bad taste or offensive?, 7th October 2016.

Cases cover a range of platforms, and the ASA has upheld cases against offensive online advertising including:

- Sexism and the objectification of women, including in ads placed in mobile games. An adult content ad featuring female nudity was placed in a mobile game by an unknown person/company[280]. An in-game ad produced by Rangosious Public Holdings depicted a player taking steps to remove a woman's clothes whilst she was asleep using an array of weapons and tools[281]. A paid-for ad on Facebook for construction machinery retailer JMac, was ruled to be sexist and offensive for its depiction of women in hard hats and bikinis[282]. These cases and other intelligence may suggest there is an issue with non-UK companies placing ads directed at UK audiences that objectify women.

- Extreme language. Banter King, an online novelty goods retailer, advertised its products in the Sky Sports app, including mugs emblazoned with expletives[283].

- Racism. The ASA has recently launched a report into the potential harms deriving from the portrayals and representation of race and ethnicity in UK advertising. While extremely rare, cases of overtly racist ads occasionally appear in paid-for online advertising. Examples are more likely to be found in organic (non paid-for) advertising content, although they appear infrequently. A 2021 ASA case upheld a complaint against an organic Facebook post from JD Recruitment depicting a woman in blackface, deemed to be racist and sexist and thus likely to cause widespread offence[284].

Example: Objectification of women

The ASA upheld a complaint against a paid-for video ad for online clothing retailer PrettyLittleThing. The ad featured multiple women wearing lingerie-style clothing in a variety of seductive poses. The complaint accused the ad of objectifying women and being overly sexualised and thus causing widespread offence, which the ASA agreed with. The ad was a pre-roll ad on YouTube seen on 29th October 2019.[285]

Figure 31: Illustration of a video advert for PrettyLittleThing

---

[280] https://www.asa.org.uk/rulings/person-s--unknown-a21-1105222-person-s--unknown.html The advertiser fraudulently identified themselves using the domain name of a well-known ecommerce site in order to buy programmatic advertising.

[281] https://www.asa.org.uk/rulings/rangosious-public-holdings-ltd-a21-1121548-rangosious-public-holdings-ltd.html

[282] https://www.asa.org.uk/rulings/jmac-ltd-g21-1126174-jmac-ltd.html

[283] https://www.asa.org.uk/rulings/banter-group-ltd-a21-1108787-banter-group-ltd.html

[284] www.asa.org.uk/rulings/jd-recruitment-group-ltd-a21-1124963-jd-recruitment-group-ltd.html

[285] ASA ruling: https://www.asa.org.uk/rulings/prettylittlething-com-ltd-cas-583039-y6l1x6.html. Image of ad available at: https://www.today.com/style/pretty-little-thing-ad-banned-uk-being-offensive-t173478

Example: Advertising involving offensive language

An ad from novelty goods retailer Banter King appeared as a display ad on the Sky News mobile app, with photos of a number of different mugs emblazoned with rude messages. The ad was seen on 27th April 2021, and faced complaints to the ASA for its use of offensive language. On the 8th September 2021, the case against the ad was upheld, deemed to be likely to cause widespread offence[286].

Legal but harmful advertising

Relative **incidence**: 🟠 Medium | Relative **severity**: 🟠 Medium | **Trend**: ⇧ Increasing

There is a broad range of legal advertising that has the potential to harm consumers, including alcohol, health treatments and cosmetic surgeries, gambling, e-cigarettes, foods and soft drinks high in fat, salt or sugar, and motoring. Adverts involving harmful depictions such as glamorising knives also fall into this category, as do ads associated with body image (see next section).

There is very limited evidence about the extent of this category of advertising, as distinct from mistargeted advertising (see section below). However, there are various examples of legal but harmful online advertising:

- The promotion of nicotine products by influencers: whilst certain nicotine products are not illegal to advertise to an age-appropriate audience, and age filters for posts on Instagram can hide certain content from users under the age of 18 (assuming they have inputted their age accurately), the promotion of nicotine products beyond treatments to help stop smoking could encourage nicotine addiction and result in smoking and the resultant health issues. 26 British influencers, with a combined 2.2 million followers, were part of a social media campaign in 2021 to promote flavoured nicotine pouches from Velo[287].

- The promotion of unhealthy foods by 'kid influencers': research by the American Academy of Pediatrics found that over 90% of food and drink products promoted by child influencers (influencers aged 3-14 years with large audiences amongst children) on YouTube were for 'unhealthy branded' products[288].

- The promotion of high-risk investments: there have been cases of influencers promoting crypto and investment schemes with no mention of the extremely high risk involved. Kim Kardashian is currently being sued by investors for her promotion of EthereumMax, a crypto currency that, at the time of the promotion in June 2021, was only one month old with unknown creators and a misleading name similar to the well-known crypto currency, Ethereum[289].

Example: nitrous oxide on social media and sponsored search advertising

Nitrous oxide, also known as laughing gas, is used medicinally for its anaesthetic and pain relief effects, and commercially as an aerosol propellant in whipped cream canisters. It is also inhaled recreationally to generate euphoria, and is the second most popular drug in the UK amongst 16 to 24 year olds, with 8.7% of Britons in that age bracket using it in 2020, equivalent to approximately 549,000 people[290]. There were an average of 4 deaths from recreational nitrous oxide use annually over the period 2010 to 2019[291]. Nitrous oxide is legal to sell for commercial purposes, but is illegal to sell for recreational use as per the Psychoactive Substances Act 2016[292].

---

[286] ASA ruling: https://www.asa.org.uk/rulings/banter-group-ltd-a21-1108787-banter-group-ltd.html

[287] The Guardian, Firms under fire for using UK influencers to push nicotine products, 8th November 2021.

[288] American Academy of Pediatrics, Child Social Media Influencers and Unhealthy Food Product Placement, 1st November 2020.

[289] BBC, Kim Kardashian sued in crypto 'pump and dump' case, 12th January 2022,

[290] Office for National Statistics, Drug Misuse in England and Wales, 9th December 2020.

[291] The Guardian, How Britain got high on nitrous oxide, 27th November 2021.

[292] Home Office, 'Home Secretary seeks expert advice on laughing gas', 3rd September 2021.

Adverts for nitrous oxide whipped cream chargers have been identified on Facebook, Instagram[293] and Tiktok[294]. The study team found an example of a 'cream charger' ad shown on Facebook and Instagram[295]. In some cases, advertised delivery times of '1 hour' and/or late evening slots, such as 5pm-2am, imply that the target market may be recreational users not the restaurant trade. Ads for 7 different providers of nitrous oxide canisters also appear in Bing-sponsored search results for 'cream chargers uk'[296], and a further 10 appear in Google-sponsored search results for the same phrase[297].

Figure 32: Google sponsored search results for 'cream charger'[298]
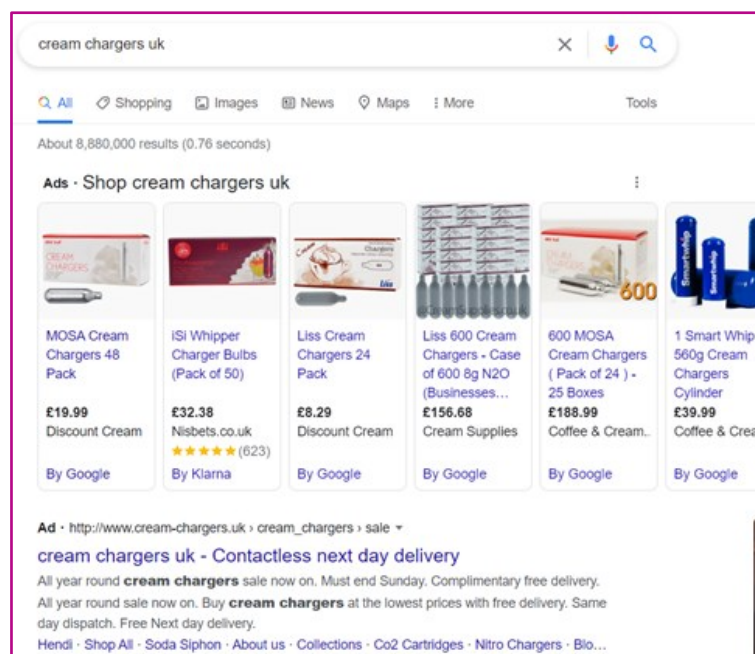
Example: Influencers promoting high-risk investments in unsafe crypto schemes

In June 2021, Kim Kardashian promoted the 'EthereumMax' coin (not to be confused with genuine Ethereum coin) to her 250+ million Instagram followers[299]. This coin was only a month old and its creators are unknown. This makes it a highly risky investment and a potential harm to unwitting consumers, who may interpret the promotion by a high-profile influencer and the name similar to that of a well-known cryptocurrency as a seal of safety.

---

[293] Spark Ninety search of Facebook Ad Library using term 'cream chargers' conducted on 03/03/2022 found 24 examples of active NO2 ads that started running in the UK over the period 01/02/2022 to 03/03/2022. None of these ads encouraged or endorsed recreational use, and all advertised it as a catering product.

[294] https://www.vice.com/en/article/m7eywy/tiktok-is-hosting-ads-for-whipped-cream-but-its-actually-nitrous-oxide

[295] Ad ID: 336567101740846 on Facebook Ad Library (from search for 'Cream Charger' on 24/02/2022). This ad went live on 23rd February 2022 across Instagram, Facebook and Messenger.

[296] Spark Ninety Bing search for 'cream chargers UK', conducted on 03/03/2022, found 7 sponsored results for providers of NO2.

[297] Spark Ninety Google search for 'cream chargers UK', conducted on 03/03/2022, found 10 sponsored results for providers of NO2.

[298] Spark Ninety Google search for 'cream chargers UK', conducted on 03/03/2022. Websites promoted by the ads include https://www.discountcream.co.uk/mosa-cream-chargers-48-pack-154-p.asp?gclid=Cj0KCQiA64GRBhCZARIsAHOLriKkGcctl-6VwOSfv36jzKavaZJeFqXT91znzM1ls-SPrkYN2tvC7tMaAiJwEALw_wcB, and https://www.creamsupplies.co.uk/cream-chargers-liss-whip-case-600, and more.

[299] FS Tech, Influencers are promoting risky and non-existent crypto tokens, warns FCA, September 2021.

Advertising contributing to body image concerns

Relative **incidence**: 🟠 Medium | Relative **severity**: 🟠 Medium | **Trend**: Unknown

Advertising can be harmful when it uses imagery and/or messaging that contributes to people's body image concerns. It may portray or present body types, cosmetic interventions or certain behaviours/lifestyles in an unhealthy way, or a way that creates undue pressure to conform.

61% of adults and 66% of children feel negative or very negative about their body image most of the time, with those at most risk of developing poor body image including early adolescents, women and girls, LGBT people and higher weight[300]. Negative body image can affect people's lives in many ways, contributing to low self-esteem; mental health conditions such as depression, anxiety and body dysmorphic disorder; a reluctance to visit the doctor, exercise or participate in activities; and the use of anabolic steroids or medication to lose weight.

The media and advertising are just two of many influences on body image, with other factors including peers, families and dating apps[301]. Although brands can have a positive influence on body image, such as the Dove Real Beauty advertising campaign, there are several ways in which advertising can contribute to negative body image, including:

- Ads involving idealised, unrealistic and/or unhealthy body images

- Ads using filtered and/or retouched images to create false impressions and mislead people

- Ads exploiting insecurities, pressure to conform, or body shaming to sell interventions

- Ads relating to body image targeted to vulnerable groups, such as under-18s

- Ad placement in harmful body image content e.g. brands sponsoring posts by influencers who present an unrealistic body image

This advertising may relate to products and services that help individuals to change their appearance, such as cosmetic procedures, weight loss, fitness, beauty, health and clothing - or in other categories of advertising.

The incidence of paid-for social media advertising that contributes to body image concerns is difficult to quantify. The majority of people reported seeing adverts on social media for weight loss organisations, gyms, shapewear, cosmetic dental treatment, non-surgical cosmetic treatment or muscle-building products during 2020. 50% of adults and 39% of young people also reported seeing adverts for cosmetic surgery[302]. However, this data does not provide information about whether these adverts represent body image in a harmful way.

The news media and blogs report issues with social media advertising relating to body image, such as repetitive shapewear advertising on Instagram[303], and growing investment in TikTok and Pinterest advertising, such as by shapewear brand Shapermint[304].

There have been issues in influencer marketing, with promoters using filters, such as those found on Instagram, to unfairly reflect the effects of certain beauty products, and thus the prevailing societal beauty standards.

---

[300] House of Commons Women and Equalities Committee, Changing the perfect picture: an inquiry into body image, Sixth Report of the Session 2019-21, 23 March 2021.

[301] Government Equality Office, Negative body image: causes, consequences & intervention ideas, August 2019.

[302] House of Commons Women and Equalities Committee, Body Image Survey Results, First Special Report of Session 2019-21

[303] https://medium.com/fearless-she-wrote/instagrams-fatphobic-and-sexist-advertising-has-pushed-me-too-damn-far-5ed9a844e74

[304] Digiday, 'Eyeballs are shifting': Why a DTC shapewear company is spending big on Pinterest and TikTok, 17 February 2022.

Example: Influencers using filters to promote beauty products

The ASA upheld against influencer Elly Norris on 3rd February 2021 for her promotion of Skinny Tan on Instagram, for using a filter in the paid promotion, distorting reasonable body image ideals in the process.[305]

Similarly, the ASA upheld a complaint against influencer Cinzia Baylis-Zullo for promoting a tanning product from We Are Luxe Ltd whilst using an Instagram filter.[306]

Figure 33: Illustration of Elly Norris (left) and Cinzia Baylis-Zullo (right) posts[307]
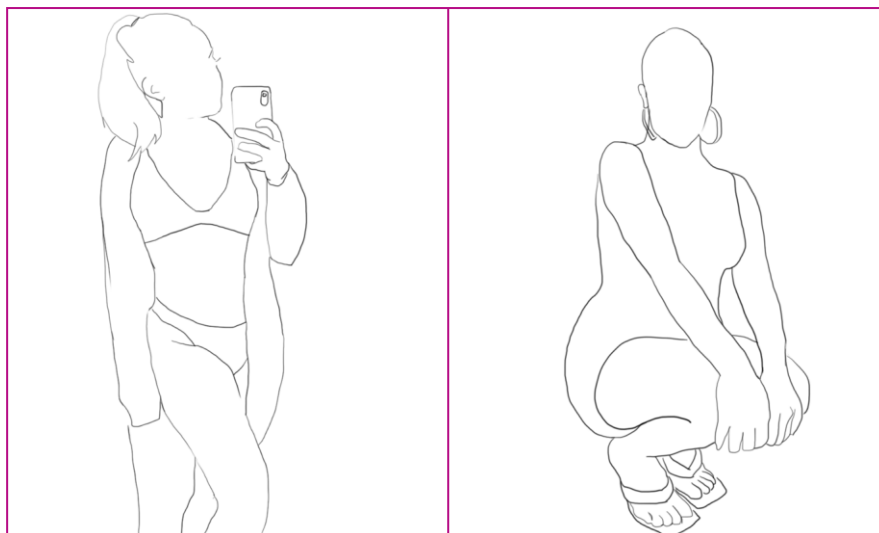
Example: social media advertising for personal training services

The following examples are 3 of 21 live ads for Ultimate Performance London City personal training services listed on Meta Ad Library in April 2022[308]. 12 of the 21 ads show "before" images, with before-and-after images available on the company's website. The ads are distributed on Facebook, Instagram, Messenger, and apps in the open display advertising market via Facebook Audience Network.

Mistargeting

Relative **incidence**: ● Medium | Relative **severity**: ● Medium | **Trend**: ⇩ Decreasing

For the purposes of advertising regulation, mistargeting involves the promotion of certain products and services to an inappropriate audience, such as age-restricted ads for alcohol or gambling served on media properties or in contexts disproportionately popular with the protected age group (children aged 15 or younger, and young people aged 16 or 17). The CAP code prohibits age-restricted ads from being directed at people under age through the selection of media or the context in which they appear, with clarification that no medium should be used to display these ads where more than 25% of the audience is measured to be under age.

Monitoring studies indicate that children continue to be exposed to age-restricted advertising on websites, apps, social media and influencer posts aimed at child audiences, though at relatively low levels. The ASA

---

[305] ASA ruling: https://www.asa.org.uk/rulings/skinny-tan-ltd-in-association-with-elly-norris.html
[306] ASA ruling: https://www.asa.org.uk/rulings/we-are-luxe-ltd-t-a-tanologist-tan-in-association-with-cinzia-baylis-zullo.html
[307] Image of these posts available at: https://www.dailymail.co.uk/news/article-9218259/Instagram-influencers-banned-using-photo-filters-boost-look-beauty-products.html
[308]
https://www.facebook.com/ads/library/?active_status=all&ad_type=all&country=GB&view_all_page_id=1742613586023834&search_type=page&media_type=all Accessed 3 April 2022.

used avatar online accounts mimicking the behaviour of young people to see if advertisers were reaching young people with age-restricted ads on YouTube channels and 49 different children's websites.

The conclusion of the reports, which ran from April 2020 to March 2021, was that, whilst the majority of online ads are targeted in line with the regulations outlined in the CAP code, there were some breaches. From April 2020 to March 2021, the ASA found:

- 101 advertisers that acted in breach of the advertising targeting rules.

- 74% of the advertisers found to be in breach of the regulations were categorised as breaching regulations surrounding the targeting of ads for food that are high in fat, salt or sugar (HFSS), with approximately half of those ads for products that are highly unlikely to appeal to children.

- 90% of the advertisers in breach of the rules were not found to breach the rules again after being contacted by the ASA regarding the issue; 10% subsequently re-broke the rules.

- The ASA worked further with the advertisers that re-breached the regulations, all of which have subsequently assured the ASA they have implemented block lists or inclusion lists to proactively address the issue and ensure that ads were responsibly targeted.

- Despite only accounting for 20% of the examined media throughout the duration of the monitoring study, 47% of the advertisers found to breach the regulations regarding the targeting of HFSS products did so exclusively on YouTube[309].

Table 24: ASA avatars monitoring of children's media: number of ads that broke CAP rules

Category	Q2 2020 [310]	Q3 2020 [311]	Q4 2020 [312]	Q1 2021 [313]
Alcohol	10	6	6	7
E-cigarettes and Tobacco	1	0	0	0
Gambling	70	5	3	29
HFSS	78	102	27	117
Weight control	0	14	11	5

A report by Nesta, a UK charity, investigated the targeting of young people with unhealthy food and drink marketing online in November and December 2021. They used 284 people living in the UK aged 13-16 to crowdsource data about the frequency and effect of the exposure of young people to potentially damaging ads for unhealthy food and drink products. They recorded 4,879 food and drink ads in the time period; 60% of these were paid-for ads, and the rest were other forms of marketing. They found:

- 70% of the ads were for products deemed 'unhealthy'.

- Over 7% of the participants were exposed to adverts for alcohol.

- Participants living in lower income households (less than £29,000 annual household income) encountered approximately 50% more ads for unhealthy food and drink products than participants living in higher income households (£29,000 or more annual household income).

[309] ASA, Protecting Children Online, 30th November 2021.
[310] ASA, Protecting Children Online Q2 2020, 26th August 2020.
[311] ASA, Protecting Children Online Q3 2020, 20th November 2020.
[312] ASA, Protecting Children Online Q4 2020, 11th February 2021.
[313] ASA, Protecting Children Online Q1 2021, 7th July 2021.

- After the data was collected, 80% of participants stated that food and drink marketing had a significant influence on their eating and drinking habits[314].

The ASA has been proactive in dealing with isolated incidents of influencers promoting alcohol/age-inappropriate products and investigating audience demographics of the influencers involved. A case against influencer Francesca Perks and Sazerac UK Ltd was upheld by the ASA, after Francesca, aged 22 at the time, took part in a sponsored social media promotion for Southern Comfort. The complaint was upheld because Francesca was under the age of 25 at the time; the CAP code states that anyone promoting alcohol in a marketing communication must be, or seem to be, over the age of 25 years old, to ensure that it is not overly appealing to young people[315].

In 2021, tests also highlighted the availability of options to target advertising to children on Facebook, though the company has since addressed this issue. The Tech Transparency Project, an online campaign for internet safety, submitted test ads to Facebook that attempted to target teenagers in the US with ads in categories such as alcohol, weight loss, pills, gambling, dating and smoking. The ads targeted interest categories, such as 'diet food' and 'poker'. It found that these ads were approved by Facebook within hours[316]. Since then, Facebook has banned all interest-based targeted ads aimed at those under the age of 18; since these changes, under 18s can only be targeted by age, gender and location[317].

Targeting vulnerable people

Relative **incidence**: 🟡 Low (limited information) | Relative **severity**: 🟠 Medium | **Trend**: Unknown

Targeting vulnerable audiences directly or by proxy may cause harm in certain circumstances. For example, gambling ads targeting individuals who have taken steps to stop receiving targeted gambling marketing communications, or fraudulent ads targeting those with a history of falling for scams. In addition, young people may be especially susceptible to influencer advertising for high-risk financial products such as day trading. 1.8 million Britons began to trade shares during the COVID-19 pandemic[318], potentially encouraged by hundreds of investment influencers.

There is very limited information about the scale of this issue. There are reports of vulnerable people being exposed to advertising that causes harm as a consequence of their vulnerability. However, there is a lack of information about whether this advertising was intentionally targeted towards them - as opposed to being targeted towards a mass audience or a broad spectrum of audience segments of which they happen to form a part.

- In 2020, anecdotal evidence suggested that gambling addicts were being bombarded with online display ads for gambling services[319].

- In 2020, there were numerous reports of young people with eating disorders being exposed to triggering adverts on TikTok. The company responded by banning adverts for under 18s that promote a harmful or negative body image[320]. Meta has also updated its advertising policies to prohibit ads that demonstrate extreme weight loss, such as 'before-and-after' photos[321].

---

[314] Nesta, Online food and drink marketing to young people, February 2022.

[315] https://www.asa.org.uk/rulings/sazerac-uk-ltd-G19-1041900.html

[316] https://www.techtransparencyproject.org/articles/pills-cocktails-and-anorexia-facebook-allows-harmful-ads-target-teens

[317] https://www.reuters.com/technology/facebook-will-restrict-ad-targeting-under-18s-2021-07-27/

[318] https://www.thetimes.co.uk/article/big-rise-in-online-share-trading-as-influencers-tempt-the-young-fxztjl0tr

[319] https://www.bbc.co.uk/news/stories-52506113

[320] https://www.dazeddigital.com/life-culture/article/50566/1/eating-disorder-sufferers-on-the-danger-of-weight-loss-ads-on-tiktok

[321] https://www.facebook.com/policies/ads/prohibited_content/personal_health

Discriminatory advertising

Relative **incidence**: 🟡 Low (limited information) | Relative **severity**: 🟠 Medium | **Trend**: Unknown

Online advertising has the power to target certain audiences, and in doing so exclude certain other audiences. This exclusion becomes an issue when it causes discrimination on the basis of protected characteristics and causes harm. Online "opportunity" advertising (jobs, credit and housing) is at risk of discrimination when targeting is used.

There is limited evidence of discriminatory targeting in the UK. In the US, an investigation by the Mark Up in February 2021 found that Google Ads services had allowed advertisers to prevent people classified by Google as gender 'unknown' (including some nonbinary and transgender people) from seeing adverts for jobs, houses and financial services[322]. Google contended that it offers users an 'Add custom gender' option and the unknown category is intended to refer to individuals where it has been unable to determine or infer the user's gender. They stated at the time that they were working quickly to resolve the issue[323]. A US report into discriminatory Facebook ad targeting found that certain marginalised ethnic groups were not being advertised housing opportunities in the same way that other groups were[324]. A report from the Centre for Data Ethics and Innovation (CDEI) found that women and ethnic minorities were being discriminated against through targeted advertising, with women less likely to see adverts for STEM jobs than men, and Asian men more likely to see adverts encouraging them to be taxi drivers compared to other ethnic groups[325]. This data may not be accurate today as it was from research conducted in 2016.

Ad fraud

Relative **incidence**: 🔴 High | Relative **severity**: 🔴 High | **Trend**: ⇨ Stable

In the programmatic open display market, ad fraud involves cyber-criminals creating fake traffic (such as using botnets to mimic real consumers), audience data, context or actions to syphon revenue from the display advertising ecosystem. Double Verify reported that in the year to April 2021 the overall global volume of fraud/sophisticated invalid traffic (SIVT), in terms of the number schemes detected and the number of devices and impressions affected, did not materially change year-on-year[326].

In the UK, Double Verify estimates post-bid levels[327] of sophisticated invalid traffic at 1.9% in the year to April 2021, a 17% year-on-year increase, compared to a 30% decrease globally from 2.0% to 1.4%. In contrast, IAS estimates that levels of ad fraud after optimisation (use of anti-fraud security solutions) are below 1% of ad impressions across desktop and mobile display formats in the UK, with a decrease in fraud levels in three out of four categories (see below).

---

[322] https://themarkup.org/google-the-giant/2021/02/11/google-has-been-allowing-advertisers-to-exclude-nonbinary-people-from-seeing-job-ads

[323] https://themarkup.org/google-the-giant/2021/02/11/google-has-been-allowing-advertisers-to-exclude-nonbinary-people-from-seeing-job-ads#:~:text=Google's%20policies%20forbid%20ads%20targeting,with%20federal%20anti%2Ddiscrimination%20laws.

[324] https://www.brookings.edu/research/solving-the-problem-of-racially-discriminatory-advertising-on-facebook/

[325] Centre for Data Ethics and Innovation, Online targeting: Final report and recommendations, 4th February 2020.

[326] Double Verify, Global Insights Report 2021

[327] Refers to SIVT/fraud levels in advertising impressions purchased, not in advertising impressions available for sale.

Table 25: Average optimised-against-ad fraud levels, UK - measured by IAS[328]

Category	H1 2019	H1 2020	H1 2021	2-year change (pp)
Desktop display	0.9%	0.6%	0.9%	0
Desktop video	0.8%	0.6%	0.7%	-0.1pp
Mobile web display	0.5%	0.5%	0.2%	-0.3pp
Mobile web video	-	0.4%	0.2%	-0.2pp (YoY)

Ad fraud has followed ad spending, with growth of connected TV (CTV) advertising expenditure leading to the emergence of fraud schemes on this platform. Double Verify estimates the CTV fraud/SIVT violation rate was 0.4% globally in the year to April 2021.

The preceding rates of invalid/fraudulent ad impressions refer to post-bid or post-optimisation and exclude any fraud that is not detected by the ad verification vendor. Levels of invalid/fraudulent ad impression pre-bid/optimisation are much higher. IAS estimates global rates of 9.4% for desktop display in H1 2021, 7.2% in desktop video, 5.5% in mobile web display, and 2.7% in mobile video[329].

Cyber-criminals are constantly adapting their tactics, devising schemes to exploit weaknesses in the ad tech ecosystem. Double Verify suggests that data centre traffic, where server-side ad insertion (SSAI) is targeted (see example below) accounted for the majority of fraud/sophisticated invalid traffic on desktop and mobile in the year to April 2021, with bot fraud having the largest share on CTV[330].

Since 2020, there has been the first conviction of a perpetrator of ad fraud, through international law enforcement action. In 2021, Aleksandr Zhukov, the self-proclaimed "Russian King of Fraud", was convicted of charges in the US, where he was prosecuted for using a bot farm and rented servers in order to create fraudulent internet traffic and inflating the cost of advertising[331]. His 'Methbot' scheme used 1,900 servers, creating millions of illegitimate ad views on major websites, such as the New York Times and the Wall Street Journal. The total earnings from the fraud were valued at $7 million. Zhukov was arrested in Bulgaria in 2018 then extradited to the US. He was sentenced to 10 years in prison by the US Department of Justice[332].

Industry has also introduced standards to help identify direct sellers and intermediaries involved in the trading of programmatic advertising inventory, including sellers.json and RTB Supply Chain Object[333]. This builds on the ads.txt standard that lists authorised sellers. These standards help buyers to identify illegitimate sellers, helping to combat certain types of ad fraud. It is unclear to what extent adoption of these standards has reduced fraud or displaced activity to alternative schemes.

The direct victims of ad fraud are advertisers who buy counterfeit advertising. Publishers are also affected due to advertisers buying counterfeit advertising instead of legitimate publisher advertising inventory. In 2020, direct losses to ad fraud were estimated to be in the range £7 million (supply chain fully optimised) to £100 million (one-third of the supply chain fully optimised and the rest non-optimised). This order of magnitude estimate is likely to still be valid, due to growth in programmatic expenditure offset by a decrease in fraud rates.

Influencer fraud is another type of ad fraud. It can involve influencers purchasing followers on social media platforms in order to give a false impression of the size of their reach online, thus allowing them to charge

---

[328] Sources: IAS, Media Quality Report, H1 2019. IAS, Media Quality Report, H1 2021.
[329] IAS, Media Quality Report, H1 2021.
[330] Double Verify, Global Insights Report 2021
[331] https://www.bloomberg.com/news/articles/2021-05-28/russian-king-of-fraud-is-found-guilty-of-online-ad-scam
[332] https://www.anura.io/blog/king-of-ad-fraud-sentenced
[333] https://iabtechlab.com/sellers-json/

artificially inflated prices for sponsored posts. Inadvertent influencer fraud may also occur, where bots use the comments sections of influencers' posts to promote their fake accounts. Whilst this does not involve deliberate action from the influencer, advertisers are still defrauded with exaggerated engagement statistics. A study by HypeAuditor in May 2021 found that fake engagement on social media could cost advertisers close to $800 million a year worldwide, and that a quarter of US influencers have more than 30% of their comments on Instagram posts from non-human, inauthentic accounts[334].

Example: 'RapidFire' connected TV fraud scheme

In 2021, ad verification company Method Media Intelligence (MMI) uncovered the 'RapidFire' scam, which allegedly generated $10 million monthly revenue, with an estimated cost to advertisers of $20 million, after considering fees and transactional costs.

The scheme used automation tools, including a Python script, to create counterfeit bid requests that spoofed CTV ad inventory across a large number of apps, IP addresses and devices. This method subverted the need for a bot farm to load apps/play content until ad breaks, making it efficient and scalable. It exploited the vulnerability of server-side ad insertion (SSAI) in common with many other fraud schemes: in 2020, DoubleVerify identified more than 12 SSAI-based fraud schemes[335].

MMI identified the perpetrators of the scam as a 5-member team of former ad tech professionals based outside the US, running an ad network called HyperCast. A fake company was registered in Nevada and appeared to operate legitimately, but this business was used to send the counterfeit bid requests to ad exchanges for monetisation through real-time bidding.

Brand safety risk

Relative **incidence**: 🟠 Medium | Relative **severity**: 🟡 Low | **Trend**: ⇨ Stable

The Internet Advertising Bureau (IAB UK) defines brand safety as keeping a brand's reputation safe when advertising online. Brands want to avoid their ads being placed next to inappropriate content, including adult, violence, hate speech, bullying, terrorism, crime, drug abuse and malware. The Global Alliance for Responsible Advertising (GARM) has developed a Brand Safety Floor & Sustainability Framework[336] identifying categories that are not suitable for any advertiser.

Brands have different preferences about where their advertising can be placed, often involving specific sensitivities, such as (hypothetically) car manufacturers wishing to avoid advertising around news about traffic accidents. The online advertising industry has started referring to the concept of 'brand suitability', which involves managing both brand safety floor risks (minimum standards) and advertisers' custom requirements.

Levels of unsafe programmatic advertising inventory/placement in the UK appear to be decreasing, though the data is not well defined. DoubleVerify found that 8.1% of UK programmatic ad impressions (measured post-bid) violated brand suitability in the year to April 2021, a 10% year-on-year decrease[337]. IAS found that 3.0% of UK desktop display pages scored were a brand risk in H1 2021, compared to 3.1% in H1 2020[338]. Over the same period, risk in desktop video decreased from 5.7% to 1.6%, mobile web increased from 3.3% to 3.4%, and mobile web video decreased from 6.3% to 2.2%. In all of these categories, only 0.1% of pages were measured as 'high' or 'very high' risk. It is not clear what thresholds and methods DoubleVerify and IAS use to identify risky content/impressions and how these have changed over time.

---

[334] HypeAuditor, State of Instagram Fraud in the USA, May 2021.

[335] https://videoweek.com/2021/10/18/are-we-making-progress-on-ssais-fraud-vulnerabilities/

[336] https://wfanet.org/leadership/garm/garm-resource-directory-%28weblog-detail-page%29/2020/09/23/Brand-Safety-Floor--Sustainability-Framework

[337] Double Verify, Global Insights Report 2021

[338] IAS, Media Quality Report, H1 2021

However, there continue to be examples of misplacement of online advertising in specific high-risk content categories, such as piracy services. Piracy websites and apps generated estimated annual ad revenue of $1.3 billion globally[339]. White Bullet identified examples of brands' advertising on these services, with brands accounting for 36% of UK ad impressions on piracy websites and 97% of UK ad impressions on piracy apps in 2021[340].

Advertising that is misplaced causes damage to a brand's reputation through association with unsafe content and can provide funding for the providers of content that is harmful to consumers and society as a whole, such as piracy and misinformation. Conversely, the reputation of legitimate publishers is at risk from placement of harmful or inappropriate advertising.

Brand safety solution vendors such as IAS, DoubleVerify, Cheq and White Bullet provide technology and tools to help brands and agencies to avoid misplacement of advertising. In some cases, advertisers have used brand safety tools in a relatively blunt way, preventing advertising placement on legitimate publisher services, thus harming publisher revenues. At the start of the COVID-19 pandemic many publishers started to block pandemic related keywords and/or news sites. Their approaches later became more refined, reducing rates of blocking legitimate publishers. DoubleVerify found that the share of brand safety violations driven by keyword blocking fell from 13% in May 2020 to 7% in April 2021[341].

Inaccurate audience measurement, attribution and reporting

Advertisers may suffer losses if they base their investment decisions on incorrect information about the audiences available to target, the audiences their ads reached, and the actions taken by these audiences as a result of seeing their advertising. In the social display market, there is limited independent verification of platform reporting data. As a consequence, reporting errors have occurred, such as:

- In 2020, Facebook discovered that data used to drive its "conversion lift" metric was in error and had affected several thousand advertisers for over 12 months[342]. This error led to a conversion lift tool provided by Facebook incorrectly reporting the incremental impact of Facebook ads on conversions (e.g. sales). Facebook offered ad credits to advertisers it determined to have been "meaningfully affected" by the issue.

- In November 2020, LinkedIn disclosed two measurement issues that led to over-reporting of some campaign metrics for impression and video views. Thus advertisers paid LinkedIn for some video views that did not occur. These issues potentially affected more than 418,000 customers over a period of more than two years. However, LinkedIn claims that 90% of these customers saw an impact of less than $25 and it offered them ad credits as compensation[343].

The scale of this issue is unclear, given limited independent verification. There are comparable issues in the open display market, though this ecosystem is more open to independent ad quality verification. Audience measurement and attribution is highly complex and there are multiple factors contributing to the emergence of issues, such as a lack of transparency and competition issues around the market power of major platforms.

[339] Digital Citizens Alliance and White Bullet, Breaking (B)ads: How Advertiser-Supported Piracy Helps Fuel A Booming Multi-Billion Dollar Illegal Market, August 2021.

[340] White Bullet, How regulation and outreach reduce ad placement on piracy websites, 2022.

[341] Double Verify, Global Insights Report 2021

[342] https://www.adexchanger.com/platforms/facebook-conversion-lift-measurement-issue-goes-undetected-for-12-months/

[343] https://www.socialmediatoday.com/news/linkedin-discovers-ad-metric-error-which-lead-to-over-400k-advertisers-bein/588960/

Annex 2: ASA Complaint Case Data

Figure 34: Number of ASA complaint cases relating to paid-for online advertising by category, 2021
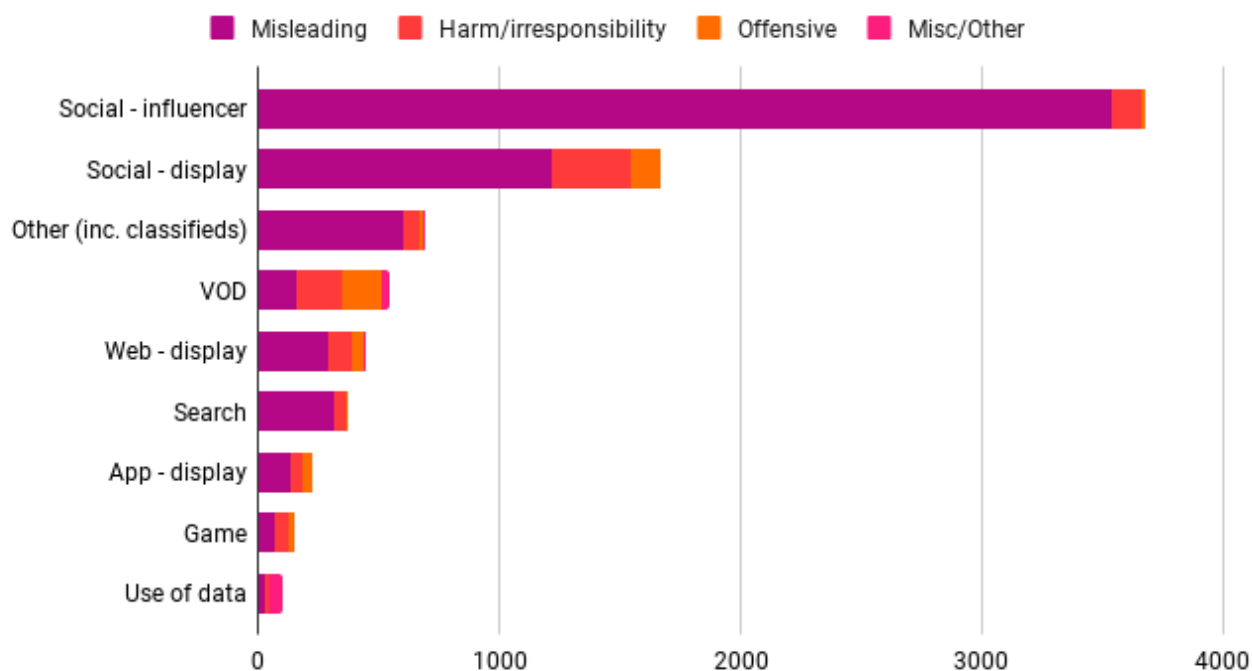
Importantly, the number of ASA complaint cases is not a direct measure of the relative levels of harm because:
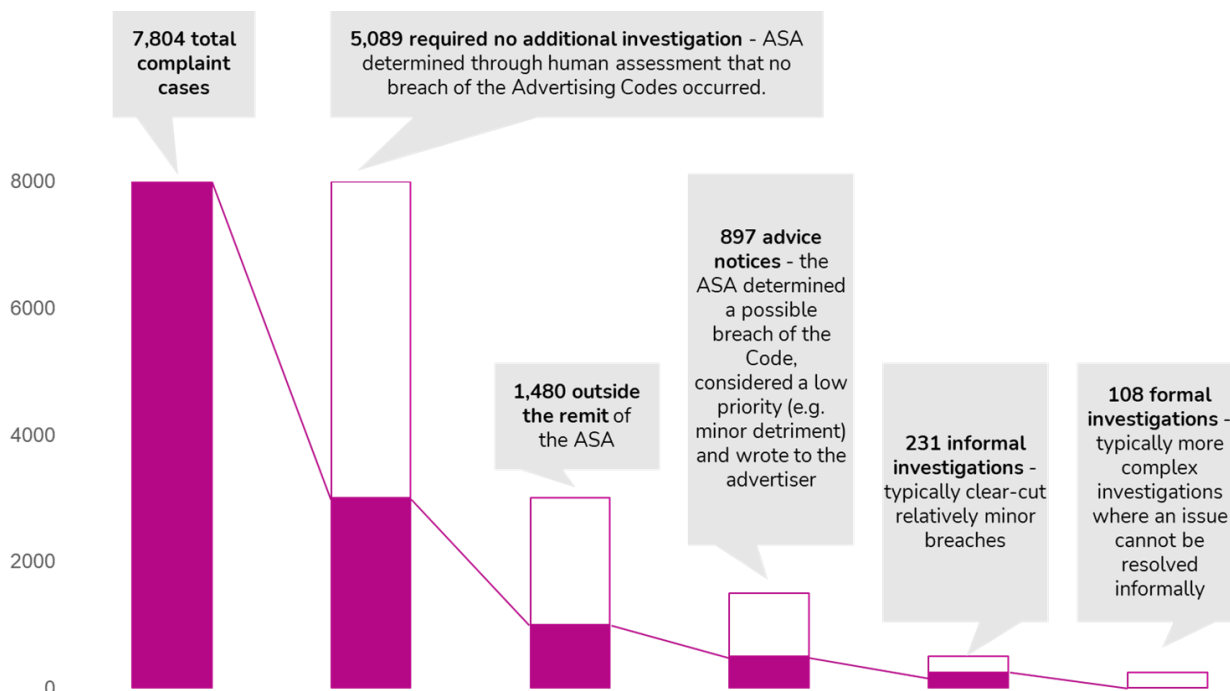
- Consumers might be more likely to complain about some forms of potential harm than others.

- Not all ASA complaint cases involve harm: only 16% of complaint cases relating to paid-for online advertising resulted in an advice notice or formal/informal investigation, with 84% being outside the ASA's remit or where the ASA determined that no breach of the advertising codes occurred and no further action was required. See breakdown of complaint cases by action taken, below. The ratio of complaints to harm might differ by category of advertising.

Figure 35: Number and growth of ASA complaint cases relating to paid-for online advertising by category, 2021
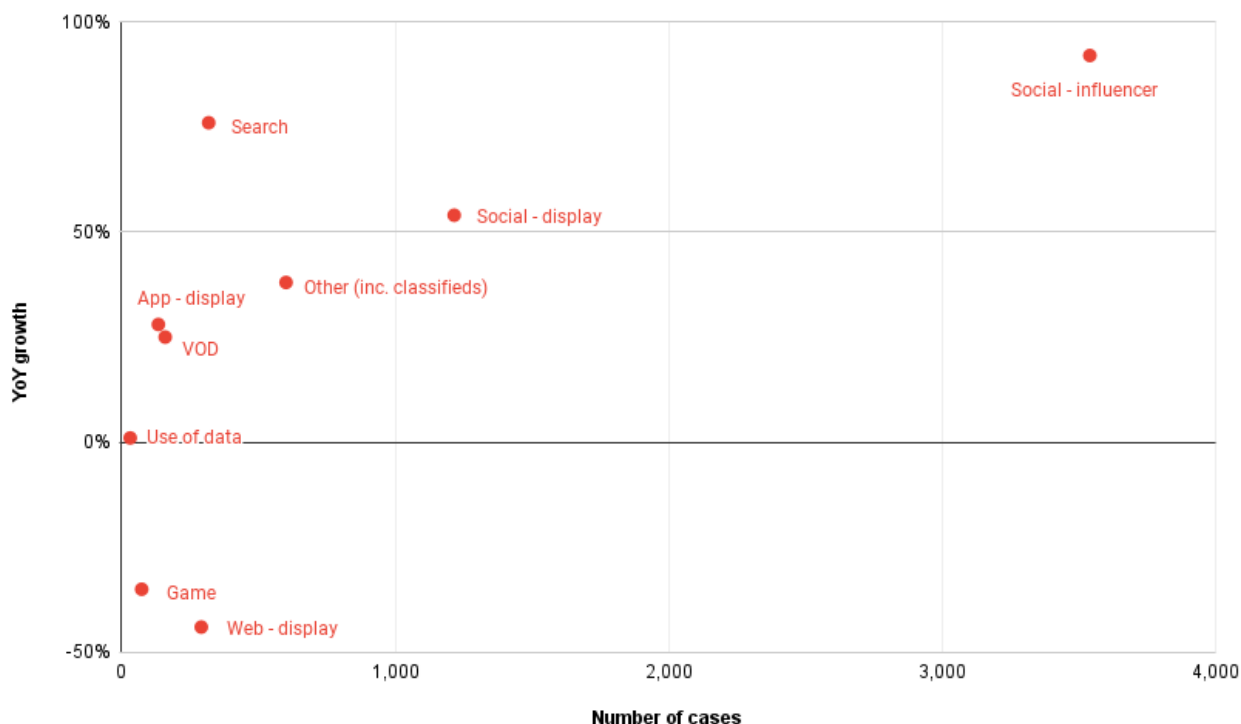
Some trends may be driven by the Covid-19 pandemic and not be representative of long-term patterns. It is also possible that the propensity of consumers to complain about different issues changed between 2020 and 2021 which would distort the trend data.

Figure 36: Breakdown of ASA complaint cases by action taken, 2021

www.sparkninety.com