MRS Awards 2024 Winner Business Impact of the Year - UK

MRS Awards 2022 Finalist Business-to-Business Research

MRS Awards 2020 Winner Innovation of the Year

MRS Awards 2019 Winner Global Agency of the Year

MRS Inclusion Pledge

STRAT 7 JIGSAW | Ofcom

Online Advertising Pathways

Qualitative research report

July 2026

MAKING SENSE OF HUMAN COMPLEXITY

Contents

1 Executive summary

1.1 Summary of research context

Ofcom commissioned Jigsaw Research to conduct a qualitative research study to help develop Ofcom's understanding of the digital advertising landscape, including the processes, systems, and features used by online advertisers, what the online advertising platforms look like in practice from the perspective of advertisers, and any experiences or concerns about fraudulent advertising, including views on how to prevent it. For the purposes of this research, advertisers are defined as individuals or organisations (including businesses) that place paid advertisements to promote products, services, or ideas to target audiences. The research incorporated views and experiences from a range of online advertisers, including running ad campaigns internally, businesses who outsource to ad agencies as well as ad agencies who run campaigns on behalf of other companies.

1.2 Summary of key findings

Advertisers' main priority was delivering against their core campaign objective, which strongly influenced platform choice.

Secondary considerations included budget and return on investment; platform ease of use and efficiency; platform familiarity; control; customer service; and platform reputation.

For some advertisers, the emphasis on 'control' reflected a more proactive approach to safety and security. These advertisers sought greater oversight of ad placements to avoid associations with fraudulent or low-quality content, including scam ads or ads being placed on websites with reputational risks. This often led these advertisers to prefer advertising on walled garden platforms, which they said felt lower risk compared to open web or hybrid environments.

That said, there was a perceived 'illusion of choice' of ad platform.

Advertisers often felt their choices were constrained due to the perceived dominance of Google Ads and Meta. Most felt that avoiding advertising on Google Ads and Meta felt unrealistic. Meta in particular was perceived to be 'setting the standard' for the advertiser journey design and platform expectations.

Advertisers often felt that ad platforms were more focused on revenue generation than fraud prevention.

Advertisers were sceptical about whether platforms gave enough weighting to fraud prevention compared to their focus on revenue generation and protection. While safety mechanisms existed in the advertiser's user journey (account verification when setting up the account, two-factor authentication when logging in and out, AI-enabled content reviews and rejections), questions persisted about their meaningfulness and effectiveness. As part of this, advertisers doubted overreliance on AI without sufficient human oversight and felt there were inconsistencies and inequalities in the process for reporting fraudulent advertising across platforms.

Advertisers distinguished between four broad types of problematic and fraudulent activity in the online advertising ecosystem (though individual cases could sometimes fall under multiple types): sharp practice, ad fraud, scams and brand impersonation, and account takeover or 'hacking'. Each came with different perceptions in terms of salience and ease of 'policing'.

Overall, there was a sense that problematic activity in the online advertising ecosystem had become normalised. Some advertisers acknowledged potential negative impacts and consequences for them, as well as for consumers, seeing a more explicit link between problematic and fraudulent activity, the erosion of brand credibility, and therefore damage to consumer trust.

There were nuances when looking at the different types of problematic activity. Experiences of brand impersonation and account takeover (attempts and actual cases of account takeover) felt relatively common but comparatively easier to ‘prove’ and/or ‘police’. By comparison, sharp practice (e.g. competitors failing to follow industry standards) and ‘ad fraud’ (i.e. click-fraud, bots) were more salient, directly threatening day-to-day campaign success, and felt harder to ‘police’ overall.

Despite advertisers relatively frequently coming across or being a victim of different types of problematic activity, there was hesitancy about introducing new regulation in relation to prevention of fraudulent ads.

Hesitancy was driven by three factors: salience of ad fraud and sharp practice; a general perception that safety and security was getting incrementally better; scepticism and nervousness about what meaningful changes could feasibly be introduced to better police these issues without causing significant disruption to their daily work.

Advertisers felt there were two core principles to consider when making improvements: ensure any changes are not too onerous to the advertiser and ensure that ‘humans’ remain at the core.

Advertisers recognised that prevention of fraudulent advertising was important and felt there were some specific areas that could be improved. Improving the reporting process felt most important to ensure all advertisers were treated equally, reporting channels were clearer, and that AI use was balanced with human judgement. Some also recognised a need for improvements at account set up (e.g. more consistent verification of advertisers when signing up), during day-to-day account management (e.g. enforcement of multi-factor authentication when logging in and making significant account changes), and when platforms review ads (e.g. clearer reasoning provided for rejected ads).

2 Background and approach

2.1 Research background

Under the Online Safety Act (OSA), Ofcom has a range of powers and responsibilities to help make online services safer for users. The OSA requires certain online service providers to operate the service using proportionate systems and processes designed to mitigate risks associated with fraudulent advertising. Ofcom is required to prepare and issue fraudulent advertising codes of practice which will describe measures recommended for the purpose of compliance with duties to prevent individuals from encountering fraudulent advertising. This code of practice will have significant implications not only for the platforms (namely user-to-user services and search services) but also for businesses placing ads.

Current evidence highlights that online scams and fraud are widespread and can be harmful to consumers' mental and financial wellbeing. The online advertising ecosystem itself is also complex. As this evidence has primarily focused on views of consumers, there remain important gaps in Ofcom's understanding, particularly regarding the perceptions and experiences of those who pay for adverts to be placed.

In this context, Ofcom needed to understand, from the perspective of those paying for advertising online, how regulation of online ad pathways could be improved to minimise harm caused by fraudulent ads online. Ofcom also wanted evidence on how advertising systems function in practice and identify any vulnerabilities within the user/advertiser journeys.

It should be noted that any opinions on platforms in this report are the participants' own, and do not reflect the position of Ofcom or of Jigsaw.

2.2 Research objectives

The overarching aims of this research were to examine the opportunities that online advertising pathways may present for fraudulent actors, and to explore advertisers' views on mitigating these risks.

The specific objectives were to:

- Enhance and refresh Ofcom's understanding of online ad pathways, including the processes, systems, and features used by online advertisers.
- Understand advertiser decision-making around what online advertising pathways to use.
- Assess the perceived effectiveness of existing safety measures against fraudulent ads online, and views on how to avoid or prevent fraudulent advertising.
- Explore the role of further regulation to prevent fraudulent ads in the future.

2.3 Methodological approach

A qualitative approach was considered most appropriate given the complexity of the topic, the key audience groups interviewed, and the overall objectives of this project. A qualitative methodology allows for the sharing and discussion of subjective viewpoints and exploration of underlying attitudes. Qualitative research can identify prevalent opinion and even strong dissenting voices within the included participants, but it cannot quantify or provide statistical representation of the prevalence of the views explored.

In this research in particular, advertisers reflected on their personal experiences across ad platforms, which included personal perceptions of the process and features on each platform. The findings presented in this report are therefore indicative of the views of the advertisers interviewed at a certain point in time and may not be representative of other advertisers' experiences or actual platform functions and capabilities.

2.4 Fieldwork audiences and methodologies

This research was split into two distinct phases: a digital task conducted via the STRAT7 Whycatcher digital research platform, followed by 45-minute, one-to-one in-depth interviews conducted via Zoom. All participants interviewed worked professionally as advertisers in some capacity, which may in part inform their perceptions of the advertising landscape and their appetite for further regulation. Fieldwork began on November 21st, 2025, and finished on January 21st, 2026.

Participants were grouped into four distinct 'audience' groups, based on factors such as business size and whether they managed their advertising in-house or via external agencies. Audience definitions can be found below.

Each audience group went through a slightly different research process, tailored to their advertising practices:

- 40 x participants took part in a digital task with questioning tailored to the audience context and advertising experience.
- Follow-up interviews were then scheduled with 25 x participants, dependent on business size, advertising approach, and audience group.

Audience definitions, their tailored methodology and how each audience will be attributed in this report can be found below. See Appendix 7.1 for detailed sample breakdown.

Audience	Follow-up interview methodology	Quote attribution used in this report
3x Businesses who outsource their ad campaigns to external companies or ad agencies.	A short 15-minute digital task focused on their advertising choices, including why they outsource their advertising. None of these businesses were invited to take part in a follow-up in-depth interview as they did not have firsthand experience	'Business who outsources'
25x Micro, small, and medium businesses who run ad campaigns themselves.	A longer 40–60-minute digital task following the live set-up of an ad campaign, including their processes, experiences, and perceptions around the platform. They were also invited to share screenshots of their journey to help illustrate their experiences and processes. 14x of these businesses were invited to take part in a 45-minute follow-up in-depth interview.	'Micro Business' (1-10 employees, including sole traders) 'Small Business' (11-50 employees) 'Medium Business' (51-249 employees)
8x Large businesses who run ad campaigns themselves.	A shorter 15-minute digital task exploring their advertising choices, including retrospective descriptions of ad setup and processes. All of these businesses were invited to take part in a 45-minute follow-up in-depth interview.	'Large Business' (250+ employees)
4x Ad agencies who run campaigns on behalf of other businesses.	A 30-minute digital task exploring their advertising choices, such as any preferences they or their clients tend to have. All of these businesses were invited to take part in a 45-minute follow-up in-depth interview.	'Media Agency'

2.5 A note on language and terminology

The participants in this research were recruited and interviewed based on their profession and were instructed to answer questions within this capacity. As a result, this report will refer to them as 'advertisers' rather than 'participants' from this point onwards. Advertisers are defined as individuals or

organisations (including businesses) that place paid advertisements to promote products, services, or ideas to target audiences.

During this research, advertisers spoke at length about their experiences and perceptions of specific advertising platforms, which are directly named in this report. These findings reflect advertisers' own accounts and should be understood as reflecting their own perspectives. The findings are not intended to establish factual claims or the 'whole truth', of platform functions, capabilities, layout, or security measures. The findings are rooted in how platforms were *perceived* by advertisers, rather than 'objective' facts.

These findings are also reflective of when the fieldwork took place. Given the fast-moving nature of the advertising ecosystem, aspects of the landscape may have changed since the research was completed.

Advertisers were recruited to reflect use of a range of ad types as well as ad ecosystem models. Where relevant, this report will call out differences between ad types and ecosystem models (types of and definitions for which can be found at the bottom of this section). However, this report seeks to reflect the language used by advertisers wherever possible. As advertisers rarely, if ever, spoke using the ad type and ecosystem model terminology when discussing their advertising strategy or decision-making, the report will refer to individual platform names most frequently.

A table with definitions of some of the more technical and common terms used in this report can be found below.

Term	Definition
Ad types	
Search Ad	Ads that appear on search engine results pages (e.g. Google or Bing) when users enter relevant keywords, typically marked as "sponsored" or "ad."
Display Ad	Banner or image-based ads shown across websites, apps, or social media platforms.
Classified Ad	Ads listed/posted on dedicated sections of websites or publications (e.g. Facebook marketplace, Craigslist, Gumtree, Autotrader).
Boosted Content	Content which looks like a user's post, but where the user might have paid the service, so it is 'boosted' or 'promoted' more widely beyond their followers. These posts might have a label that says they are an 'ad' or 'sponsored'.
Ad ecosystems	
Walled Garden	Ads sold and placed by one platform – so the platform is responsible for collecting data on impressions and audiences, inventory management and targeting. For example, Facebook ads run through Meta Ads Manager.
Open Web	Ads that are placed by external services across a range of independent websites and apps. For example, using 'The Trade Desk' to place banner ads across news websites, blogs and forums.
Hybrid	Ads that are placed via classified ad networks which distributes them across multiple partner websites or apps. For example, running ads through Gumtree that are published across other partner websites.
Security mechanisms	
Multi-Factor Authentication (MFA)	Security checkpoint which requires users to provide at least two forms of identification in order to access an account, most often when logging into the account.

Two-Factor Authentication (2FA)	A sub-set of MFA in which a user must provide two forms of identification to access an account or complete some action. Some forms of authentication mentioned include an account password, a code emailed or texted to the user by the platform or a verification app with a unique code display. *Note that advertisers often used the terms '2-FA' and 'MFA' interchangeably.*
Problematic activity in the online advertising ecosystem	
Fraudulent advertising	Scam ads that could mislead customers, for example, a scam or impersonation of a company's brand. *Note: The definition provided was used specifically to ensure participants understood the difference between fraudulent advertising and ad fraud.* *Note: Advertisers' views on what constituted a fraudulent advert were not always aligned with legal definitions, and in some cases encompassed practices that would not amount to fraud under the UK fraud offences or the OSA.*
Ad fraud	Websites, apps, or bots creating false interactions like clicks or impressions to generate revenue from an advertiser.
Sharp Practice	Advertising that may be ethically dubious or 'pushing the boundaries' in terms of legally permissible behaviour. For example, failing to follow industry standards, having branding that is very similar to colours/fonts used by other brands and so on.
Scams	Deceptive ads designed to mislead consumers into parting with money and/or personal information.
Brand impersonation	Unauthorised use of significant elements of an advertisers' own brand by another party, including directly and overtly copying brand names, distinctive colours, logos and other recognisable assets without permission.
Account takeover or 'hacking'	'Bad actors' logging into advertising accounts, locking legitimate users out, potentially using the account to run scam ands and/or in the worst cases, threatening the organisation with ransom demands in order to restore access.

3 The Ad Ecosystem

3.1 Section overview

This section examines advertisers' decision-making processes regarding platform selection and perceived roles different platforms play within the advertising ecosystem. The section details the step-by-step journey advertisers follow to launch campaigns across platforms, from account set up through to campaign launch along with advertisers' assessments of these processes. The existence of and feelings toward artificial intelligence (AI) tools as part of the ad ecosystem is also explored in detail.

3.2 Advertiser decision-making

3.2.1 Factors driving platform choice

Advertisers often weighed up various interlocking factors when deciding which platform to advertise on, including:

- Campaign objective
- Budget and return on investment
- Platform ease of use and efficiency
- Control
- Perceived platform dominance and familiarity
- Platform reputation
- Customer service

Achieving the campaign objective was the most prominent driver of platform choice. The remaining factors were considered in relation to one another with some nuance by audience, but without a strong hierarchy of importance. The below sections explore each of these factors in more detail.

Overall, whilst elements of 'customer service' and 'platform reputation' had some connections to the safety and security of the platform itself, prevention of and/or protection against fraudulent advertising was not consciously considered as a key decision driver.

3.2.1.1 Campaign objective

Advertising on a platform that would ensure the advertiser could achieve the campaign objective was always the top priority. Typical campaign objectives included:

- Brand awareness: introducing a brand to a new audience
- Product/service consideration: deepening engagement with the brand as well as its products/services amongst new and existing audiences
- Converting sales: facilitating a smooth journey from product discovery to purchase via strong visibility at key touchpoints, such as appearing as a top result for keyword searches in major search engines (i.e. Google, Microsoft Bing).

Advertisers often mapped their core objective against platforms to assess their suitability, this included exploring several aspects including:

- **Audience reach: assessing** whether the platform enables effective targeting and reach of desired audience.
- **Quality of conversions**: ensuring maximal, high-quality impressions/clicks rather than only quantity.
- **Product fit**: assessing whether the platform audience and focus aligned with the advertisers' brand/product alignment, for example, B2B (business-to-business) businesses may be more likely to advertise on LinkedIn.

> *It all depends on the goal. For example, if we were to launch something on the dealer side of the business, we'd want to look at Google Ads to consider – is their search volume in key words that might be relevant?*
>
> **Large Business**

> *If I'm looking for more like a professional, more of a sort of CEO/founder market, I'm going to go for LinkedIn.*
>
> **Micro Business**

3.2.1.2 Budget and return on investment

As with any business decision, advertisers had to consider the budget they were working with when deciding on platform. Often advertisers referred to this as 'cost per click' or 'cost per engagement'. Quality of the engagement far outweighed quantity when assessing which platforms provided best 'value for spend'. Advertisers sought to discount 'bot' impressions when assessing genuine campaign engagement and results, though advertisers could not always verify which impressions were legitimate or bots due to lack of transparency.

Overall, ads bought via open-web inventory (often accessed through platforms such as Google Ads) were perceived as more expensive than those delivered in walled-garden environments (e.g. Meta Ad Manager). This was often tied to advertisers' concerns that open-web environments carried a higher risk of 'bot' or 'poor-quality' impressions, leading to greater cost for lower-quality engagement.

Google Search ads were referenced as particularly expensive and if included in an advertisers' strategy, could take up most of their ad spend. Part of this high cost was associated with the 'bidding' nature of keyword searches, and the fact that advertisers would have to effectively 'out-bid' each other for higher placement in search results. This was felt to make it more challenging for lesser-known brands to 'compete' in this environment given the investment required to have traction.

> *We've done bits on Snapchat, bits on Instagram. They haven't always worked because I think you have to go big or go home with those kinds of channels. Unless you've got budgets of multi-tens of millions to cover every single touchpoint, you are just shouting into a thunderstorm a bit.*
>
> **Large Business**

3.2.1.3 Platform ease of use and efficiency

The ability to quickly and easily launch a campaign mattered strongly to all advertisers. However, it was particularly important for sole traders and micro businesses. These audiences typically had less specialist advertising expertise and were managing marketing alongside multiple other responsibilities, increasing the importance of choosing platforms that felt easy to use.

Once advertisers had learnt the set-up process on one platform, they tended to lean toward platforms that followed a similar flow to avoid having to re-learn an entirely different process. Meta Ad Manager was often cited as the starting point for learning the process due to existing platform familiarity through personal

accounts and perceived overall platform dominance, and as a result, advertisers perceived Meta Ads Manager to set the standard for other platforms.

Advertisers also gravitated toward platforms that offered features or tools that enabled efficiency in the process. Examples of such tools included:

- AI integrations that support with designing ad creatives (e.g. recommend text descriptions)
- Automated and intelligent targeting capabilities, including AI targeting
- The ability to 'duplicate' existing campaigns.

Meta Ad Manager was again often referenced as leading the way in terms of offering features and tools that enabled advertisers to find efficiencies in the process without diminishing campaign success.

> *If you use Facebook, every other social interface is pretty much the same. So, you don't need to sort of re-learn anything.*
>
> **Micro Business**

3.2.1.4 Control

Control over ad placement, ad content itself, spend, and targeting was a key consideration, especially for those in specialist paid-media roles working in media agencies or in medium and larger businesses. These advertisers tended to have in-depth knowledge about the intricacies of the advertising ecosystem and stronger opinions about what they felt would be effective or not for achieving their campaign goal.

A frequently cited example of where control was factored into advertiser decisions was when advertisers considered where to place the campaign in terms of advertising model (open web versus walled garden versus hybrid). Advertisers often felt that open web and hybrid environments had potential to introduce more risk (i.e. the ad appearing on sites they did not approve) and afforded advertisers with less control.

For example, some felt it could mean an ad is placed on less relevant, or even inappropriate websites. Advertisers felt this could then generate poor engagement quality and even, for larger well-known brands, bring negative reputational implications on the advertising company. Most tended to prefer using platforms that operated within a walled garden as they felt this environment provided greater control and transparency over where their ad would show up.

> *Some of the elements of the audience networks…for context, this is where your ads can be shown on websites of other businesses or websites that partner with the ad platform. So, for example, someone might see a LinkedIn ad on a random news site like CNN…I try to minimise using that sort of thing as much as possible. I switch that functionality off on all platforms because you see a lot of poor-quality clicks that come through. You're just trying to keep as much of a handle on it as you can.*
>
> **Large Business**

Control and transparency over campaign performance and engagement data also mattered significantly to advertisers of all types and sizes. This included oversight of aspects such as:

- Quality of engagement (impressions and click data) to screen out bots
- Feedback on which ad image/text combination performed best/worst
- Detailed data around audience targeting

Advertisers' access to this type of data facilitated a sense of control, enabling advertisers to learn from and amend the campaign approach in current and future campaigns to maximise the campaign objectives. It was also seen as useful for evaluating ROI or 'value for spend' on an individual platform.

However, control and transparency over campaign performance and engagement data could be de-prioritised where other factors felt more important, such as platform familiarity. This is explored further in Section 3.2.1.5 below.

3.2.1.5 Platform perceived dominance and familiarity

Certain platforms were perceived to hold dominance in the advertising market by virtue of their perceived dominance in the consumer market; the two most significant being Meta and Google Ads. Advertisers often felt this perceived dominance made it difficult for them to run successful campaigns without including some 'ad spend' on at least one of these platforms.

Advertisers cited several reasons for this, including:

- **High user base**: these platforms were perceived as having an extremely high number of regular users, which meant, for most brands, advertisers could target a larger proportion of their audience on these platforms than on any other single platform.
- **Personal familiarity**: advertisers were often also personal users of these platforms (e.g. they regularly see Google Ads, have Facebook/Instagram accounts, etc). They were therefore familiar with their layout and interface as consumers and in the case of Meta in particular, could easily integrate their advertising account with personal accounts if desired.
- **Competitor presence**: advertisers reported that competitor brands advertise heavily in these spaces so if their brand did not appear in these spaces, it could feel like a critically missed opportunity.

In some cases, the perceived dominance of Meta and Google Ads superseded the importance advertisers placed on other factors. For example, Meta and Google Ads were felt to offer little transparency and control over engagement data but advertisers felt that they had to use these platforms anyway due to the above reasons.

> *As I'm sure you know, or lots of people may have told you, they [Google Ads and Meta] basically have monopolies. What is our option really? We're not going to invest everything in [competitor platform].*
>
> **Large Business**

3.2.1.6 Platform reputation

The public reputation of a platform was factored into advertiser decision making. There was a sense that by virtue of advertising in the space, their brand would be associated with the platform itself. Advertisers therefore gave some consideration to whether a given platform aligned with their brand values or campaign goals.

The primary platform mentioned by some advertisers as being perceived as potentially risky to advertise on was the social media site or app, X (formerly, Twitter). Some reported actively avoiding advertising on X as they felt their brand values were misaligned to the platform values and did not want their brand associated with it.

Other platforms, such as YouTube and TikTok Shop, were sometimes perceived as hosting poorer quality ads that felt like 'scams.' Advertisers were therefore reticent to advertise within these platforms as they did not want their brand associated with ads that felt less legitimate. See Section 4 for more detail on how these perceptions map onto perceived safety and security of the platform itself.

> *Every time I'm on Twitter, most ads on there feel like a scam. They don't really feel relevant to me.*
>
> **Medium Business**

3.2.1.7 Customer service

Customer service had some influence over advertisers' platform choice, but to a slightly lesser extent than some of the other factors explored above. Larger businesses and media agencies more often referenced the importance of customer service, wanting quick and easy access to human customer service agents that could offer guidance or support. This felt particularly important when they are facing issues, for example, their ad has been rejected, or they are locked out of their account.

Advertisers reported that across multiple platforms (and at least Meta and Google Ads), human customer service was typically only available for businesses hitting minimum spend thresholds, which can be prohibitively expensive for small and micro businesses. An exception to this was TikTok, which advertisers perceived as offering strong account management support.

> *[Platform account managers generally] are very much there to get you to spend more money with them.*
>
> **Small Business**

3.2.2 How advertisers see the role of platforms perceived as most dominant

As referenced above, Meta and Google Ads were perceived as the most dominant platforms by advertisers.

Overall, Meta and Google Ads were felt to deliver against the following:

- **Campaign objectives**: Meta for 'discovery' based ads and Google Ads for 'conversion of sales'.
- **Efficiency** and ease of use: Meta was felt to 'set the standard' in terms of the set-up journey and sophistication of tools, particularly those for audience targeting. Google Ads was referenced for similar reasons, including tools to support with efficiency, such as automated text optimisation.
- Return on investment: while both platforms were considered relatively expensive (particularly Google Search ads), advertisers felt that more often than not, they delivered on the campaign objective.

Advertisers did however have some hesitations about both platforms, including:

- **Control**: whilst advertisers felt both platforms provided some sense of control over where ads were placed, the platforms were felt to provide low visibility over engagement data[1] (impressions and clicks) and targeting algorithms used, which inhibited them from adapting or amending their campaign approach to better suit their needs.
- **Customer service**: both platforms were felt to have limited access to human support and slow processes for resolving customer service issues, particularly for those with lower ad spend.
- **Platform reputation**: both platforms were perceived to be 'monopolising' the ecosystem which could raise some ethical concerns; by virtue of their perceived dominance, advertisers felt these platforms were not incentivised to offer transparency and 'value-for-money'.

[1] Engagement data, from the advertisers' perspective, includes both impressions data which is the total number of times an online ad is displayed on a users' screen and click data, which is the number of times users clicked on an ad.

Despite this, hesitations were minimised based on the platform strengths, and ultimately, most advertisers felt they could not realistically avoid advertising on Meta and Google Ads. The below sections deep-dive on each platform.

> *So, in terms of spreads, Google and Meta are the powerhouses. So that is where let's say probably like 90% combined of the, the total investment goes on those… Google and Meta being the primary ones now like I said before because Meta is slightly more cold audience, those customers are worth less to us, but we can drive a whole load more. So, if anything, we get like we get a larger portion of signups coming from Facebook. Google is, we take Google customers, we acquire them at a higher CPA [cost per action], but we know that they, they have more intent, they have a better retention rate and so actually they make us more money in the long run.*
>
> **Medium Business**

3.2.2.1 Meta

Most advertisers reported using Meta for 'discovery-based' ads, with the purpose of meeting audiences 'where they are' to build brand and product awareness and generate interest.

Given the perceived dominance of both Facebook and Instagram as social media platforms ('it's where audiences are'), advertisers had a sense that not advertising in these spaces would be a missed opportunity. While Meta was seen as a more expensive platform, advertisers felt it delivered value-for-money.

> Facebook really is the bread and butter. It used to be a lot easier… to be able to spend a lot less money for a lot better results. But of course, like everything, it's now very saturated. You've got to spend a decent amount to get what you want out the end of it, to be honest.
>
> **Micro Business**

Meta was also seen as offering strong AI tools for efficiency and targeting, such as Advantage+ and Lookalikes (audience targeting). Advertisers also reported that Meta provided them a sense of control over their campaign, allowing them to, for example, 'turn off' Meta's 'audience networks' to prevent their campaign showing up on sites that felt less aligned to their brand. However, they were seen as offering lower visibility over output data, such as impressions, and the algorithms they use to optimise targeting. Compared to Google Ads, advertisers felt that Meta was less proactive against 'bad actors' and that it was an easier environment to impersonate brands and appear legitimate, as their ad review process was felt to be less stringent.

Larger businesses with spend over a certain threshold reported having a dedicated account manager who could facilitate them if any issues arose. However, smaller businesses that did not meet that threshold and therefore lacked an account manager felt Meta lacked robust customer service channels. Many of these businesses said they struggled to access human support when they needed it and were subject to lengthy processing times.

> *And then Facebook, only if you're big enough, you have an account manager. Otherwise, it's all help articles, AI chat bots, and all like that. It is insanely frustrating to get anything done in Facebook unless you're basically a mega spender with them.*
>
> **Small Business**

3.2.2.2 Google Ads

Advertisers said they primarily turned to Google Ads for campaigns designed to 'convert sales', by responding to a user's specific search or need. Google Ads is the primary search engine for the public, so advertisers sought to have a strong presence. That said, the barrier to entry was seen to be high and many advertisers reported that organisations had to invest significantly in order to reap the benefits. When an advertiser was able to invest sufficiently, they felt Google Ads was a platform that would deliver on the campaign objective. Nevertheless, the high barrier to entry was perceived as prohibitive for smaller brands, making it harder for them to compete.

> *It's just very expensive and I think it's so competitive and you get, you know, you get the big conglomerates and corporations who can kind of get the lion share and you're kind of left scrambling for the scraps and it's, it's not as easy.*
>
> **Micro Business**

When assessing the usefulness of the Google Ads' tools, features and functionalities, advertisers had mixed views. Some advertisers found their AI tools helpful, particularly where the tools could streamline the creative process (e.g. AI-generated copy or imagery). However, others were wary about over-use of these tools, as it could risk generating creatives and copy that go against their brands' guidelines or regulation. This was particularly true for larger, more well-known brands as well as advertisers in finance and medical industries, due to additional regulations within these industries.

Much like Meta, Google Ads was felt to offer lower visibility over output data, such as impressions, and the algorithms they use to optimise targeting, and advertisers also felt the customer service was lacking through slow and limited human support.

That said, advertisers perceived Google Ads to have stricter policies to protect against fraudulent advertising or 'bad actors', including stronger policies about what advertisers can or cannot say in regulated sectors and overall stricter compliance requirements. Advertisers pointed to more frequent flagging or pausing of campaigns as evidence for that. Sections 4 and 5 explore this in more detail.

> *Google smart bidding has been doing that [incorporating AI] for upwards of four or five years, probably even much more. And anyone who's a marketer like me and sort of claims to understand it is lying. And that's the point. It's, you know, it's a black box for a reason.*
>
> **Large Business**

3.2.3 The role of other platforms

When advertisers ran campaigns on other platforms, this was typically done to meet a specific campaign objective, such as to reach a particular audience or direct traffic to a secondary marketplace. It was also typically an auxiliary channel to their Meta or Google Ads campaigns.

This report spotlights some of the more commonly mentioned platforms aside from Meta and Google Ads, as well as some less common platforms but which provide specific or niche capabilities for advertisers.

3.2.3.1 LinkedIn

Advertisers typically turned to LinkedIn for B2B products or brands, and to reach senior decision-makers.

The platform was also felt to be credible and trustworthy; “the professional social media site designated for professional audiences”. This was aided by the perception that the platform generated better quality B2B leads than others.

Advertisers also felt they had a stronger sense of control over their campaigns than on other major platforms, with the option to toggle features on/off to suit their needs.

> *We target a B2B audience, so LinkedIn suits our needs and means we can easily define and pinpoint our target audiences and personas.*
>
> **Business outsourcing to ad agency**

3.2.3.2 TikTok

TikTok was seen as the platform where advertisers could reach younger audiences and generate ‘organic’ brand engagement through boosted content. For most advertisers, TikTok was often a secondary or auxiliary platform.

The exception to this was some micro-businesses who sold directly on TikTok marketplace due to the perceived lower barrier to entry, as businesses can sell their product via TikTok shop, and advertise on the platform with smaller budgets and limited training. For other advertisers, there was a perception that the sheer quantity of brands and users on the platform could mean ad spend would need to be high to ‘cut through the noise’ and the return on investment was not always guaranteed (unlike on Google Ads, which was perceived as a more guaranteed way to provide a high return on investment).

Advertisers who engaged with TikTok also reported strong account support including guidance about how to set up campaigns and dedicated account managers regardless of ad spend.

> *I’m on an advertising journey in terms of what I can do. I’m using TikTok because it’s easy and accessible in terms of reaching a wide audience and selling the product on the platform itself.*
>
> **Micro business**

3.2.3.3 Spotify

Spotify was seen as offering highly specific audience targeting based on behaviours, attitudes, and location, which could be particularly useful for advertising location-specific events and services. Spotify

could also uniquely catch people ‘on the move’ via audio engagement and would not be reliant on consumers scrolling or searching online to reach them.

Spotify was seen as a cost-effective way to build traffic and awareness, in particular contrast to Meta and Google Ads. It was also described as easy to use, though there was some concern around ‘conversion building’ (i.e. converting audiences into customers) and ‘tracking’ (i.e. ensuring individual campaigns are connected to performance data).

> *You target a mass volume of users. It gets people on the move. It’s easy enough to set up with the exception of conversion building and again, it’s very cost effective.*
>
> **Medium business**

3.2.3.4 Microsoft Advertising

Microsoft ads fulfilled a similar purpose for advertisers as Google ads – ads to convert sales by responding to a consumers’ specific search or need, but at a fraction of the cost. The Video and Connected TV (CTV) offering within Microsoft advertising was also specifically referenced to capture audiences on streaming sites, enabling advertisers to post video ads which felt more dynamic and engaging. Microsoft was also felt to offer strong performance data outputs that allow advertisers to learn and improve future campaigns.

That said, Microsoft (especially when setting up CTV campaigns) was felt to perform less well in terms of ease of use, with the set up considered less user friendly than Meta and Google Ads, slow review processes (i.e. campaigns taking a long time to be reviewed before they could go live), and lesser reach compared to Google Ads.

> *It’s not user-friendly, but once you know how to do it, you save significantly on your budget. I have had cost per views of £0.01 on Microsoft which is unheard of on other platforms.*
>
> **Medium business**

3.2.3.5 AppLovin

AppLovin was mentioned as the dominant advertising platform for app-based products, such as games. The platform, which is open web, works by using ‘billboard’ space on other apps to advertise.

Advertisers appreciated its automated creative tool where advertisers would upload several variations of their creatives (i.e. static, video, playable), and the platform would automatically decide what optimised combination to present to consumers. This was appreciated for time and cost savings.

However, advertisers also expressed frustration over the lack of control or transparency the platform offered regarding which apps their ads were run on or how AppLovin’s algorithm decided where to post an ad.

Similarly to Meta and Google Ads for web-based advertising, AppLovin’s perceived dominance in the app industry meant advertisers could feel they must advertise on the platform or risk losing a competitive advantage.

> *If you're not advertising there, then you're just either doing something wrong or you're definitely falling behind competition because everyone's there and everyone's spending a lot of money there.*
>
> **Small business**

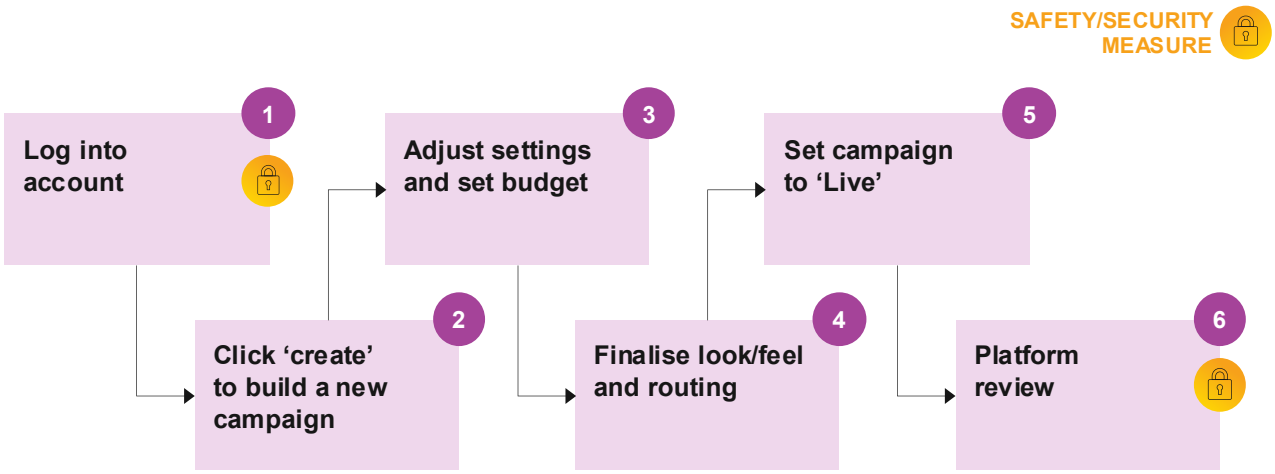
3.3 The online advertising pathway

3.3.1 A 'typical' online advertising journey

Most platforms were perceived to follow similar flows when launching a new campaign. Safety and security measures were reported as typically showing up at login stage and when the campaign was set to go live, which generally felt sufficient to advertisers.

An overview of the typical campaign flow can be summarised as follows:

Figure 1: Diagram showing the typical steps to set up an ad campaign



The flow follows six key stages:

1. **Log into account**: Most platforms offer 2-factor authentication (2-FA) when logging in, though some businesses reported that this security mechanism could be 'opted-out of' during the account creation stage. Some examples of 2-FA could include inputting the account password and being prompted to verify through a WhatsApp text, a one-time code sent to an Authenticator app (such as Microsoft Authenticator or Google Authenticator), or facial recognition. This most frequently would occur when logging into an account on a new device, or on a device that had been shut down or timed out. As advertisers reported that some platforms (including Meta and LinkedIn) allow business accounts to be linked to a personal account, which they rarely logged out of and would open pre-logged-in on their personal or work devices, they would often face no security screening at all.
2. **Click 'create' to build a new campaign**: At this stage, advertisers typically defined the campaign goal, created ad sets, and named the campaign.
3. **Adjust settings and set budget**: Next, advertisers would define and set targeting preferences, including date/period, as well as set the budget for the campaign. Advertisers reported several potential AI opportunities at this stage, with some platforms offering AI-driven targeting or algorithms to maximise utility of spend. For some platforms, advertisers said these settings would be the platform's 'default' and they would have to actively switch them off if they didn't want to use them.

4. **Finalise look/feel and routing channels (i.e. where the ad links to)**: Advertisers upload any ad copy or creatives, including imagery, videos, text input, and URL link to ad. Some reported AI integrations at this stage, primarily around optimising the ad copy (i.e. adjusting size or recommending caption text).
5. **Set campaign to 'Live'**: Advertisers review final details of the campaign, including budget, targeting, timing, etc, and then set the ad to go live.
6. **Platform Review**: Once set to live, advertisers report that most platforms enter the campaign into a 'review' phase before it is officially launched. Most presume this is powered by AI rather than humans, and advertisers note that this is where an ad may be rejected or delayed.

> *The steps I take are set up the campaign; ensure all settings and targeting are correct; add in ad variations and copy; launch campaign and scale in line with performance.*
>
> **Large Business**

> *I find it somewhat easy to set up. It takes about 15-20 minutes when there is just one creative to upload.*
>
> **Small Business**

The Meta platform journey was considered the 'standard' approach to campaign set up. Advertisers felt the platform flow felt familiar and "easy to use".

Below is an example from a Medium Business launching a campaign on Meta Ads Manager using a Business Account.

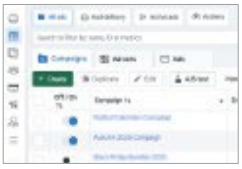
Figure 2: Diagram showing the steps to set up a campaign on Meta Ads Manager

SAFETY/SECURITY MEASURE

Log into account – 2FA required 1

> ***When I log in, I have to do a 2-factor authentication to make sure it's me.*** *I login with my password and then I get a passcode to my app on my phone.*

Create campaign and set goal for the ad 2



Adjust campaign settings and set budget 3

> ***Next, I set things like the budget, campaign objective and if I want to use 'advantage catalogue plus ads'…*** *I also have the option to select if we fall under the 'special categories' but we do not as this is primarily political ads or finance related ones.*

Set ad group: choose name, target audience, profiles, location 4

Upload chosen media and supporting text 5

Add URL and publish – ad is 'reviewed by Meta' before going live 6

> ***…then I can hit publish and the ad will be reviewed by Meta before going live.*** *There are no additional checks.* ***Sometimes I get a warning about the format of the ad once it's been reviewed*** *– e.g., it is not suitable for Instagram reels and then they prompt me to add another version.*

3.3.2 Friction in the journey

Advertisers tended to explain pain points in the advertising journey as ‘minor irritations’ rather than major points of friction. These centred around managing platform settings, features and tools as well as platform reviews and rejections. The below sections explore these in more detail.

3.3.2.1 Platform reviews and rejections

Most platforms were perceived to have some lag between the advertiser setting the campaign to go live and the platform officially publishing the campaign. This lag could last from a few minutes to several hours.

Most advertisers assumed the review process was largely or entirely conducted by AI, with humans only stepping in to review cases that had been appealed by the advertiser. Whilst there was a perception that AI ad reviews sped up the process overall and were therefore a good thing, many advertisers expressed frustrations that AI could be overprotective, inconsistent, and unnuanced in which ads it rejected. Advertisers reported a lack of clarity over what the platform was reviewing. Many assumed the reviews checked the campaign creatives and campaign content for fraudulent activity and alignment with regulation and community guidelines. However, this did not feel clear as advertisers reported guidelines were not easy to find or understand, and rejections could feel based on confusing reasoning. There was a feeling amongst some advertisers that reviews were driven by desire to protect the platform’s revenue (e.g. not publishing poorly designed ads that would generate few clicks) rather than as a safety or security precaution.

> *I don't think a person is reviewing it at first. I think it's AI doing it.*
>
> **Large Business**

Most advertisers reported having had an ad rejected at some point, with some reporting more frequent rejections when they were newer to a platform and had not yet worked out the precise elements they needed to avoid for their ad to be approved on that specific platform. The reasons provided for ad rejection often felt vague, written in overly technical language, and generic, making it difficult for advertisers to apply the feedback to pass the review. In the cases of ads with imagery or video, advertisers could struggle to work out which part of the ad was at fault. This could be particularly irritating for advertisers who believed there was no human resource they could contact for more information or to review the ad and therefore felt left in the dark as to what their recourse was. In some cases, the advertiser reported they could make inconsequential tweaks to the rejected ad (i.e. by removing a semicolon) and re-launch the near-identical set of creatives and text on the same platform without facing rejection; demonstrating an inconsistency in the review application and process.

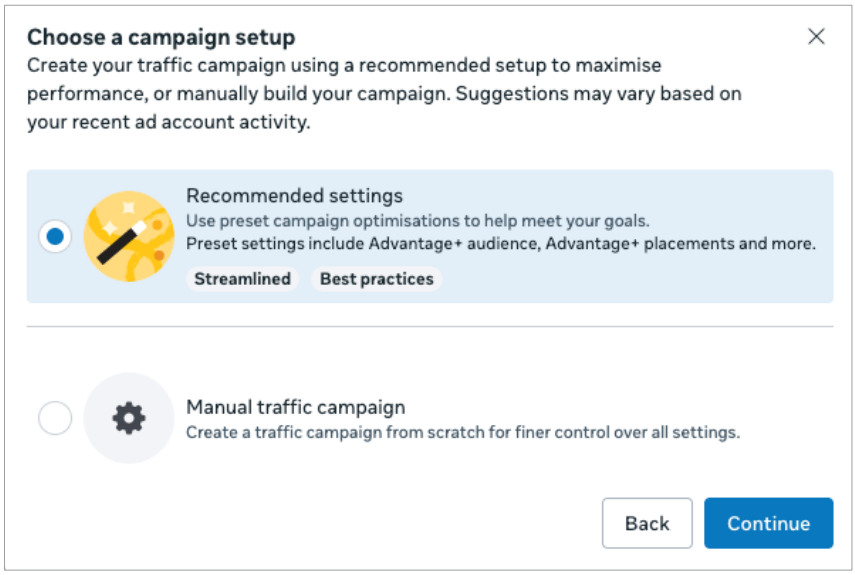
Some advertisers reported seeing live competitor ads that seemed to breach regulations or platform guidelines. For example, a healthcare brand advertising a prescription medication which went against both industry and platform regulations. This felt inconsistent with the way AI had previously enforced reviews and rejections of their own campaign content and was ultimately felt to put ‘good actor’ brands at an unfair competitive disadvantage. In some cases, advertisers attempted to report these challenges (including in more extreme cases, to industry bodies) but it felt difficult to know who to report to and how.

> *We did get flagged for violence, but we were talking about a game that had no blood… It was just a stickman fighting another stickman. And they just kind of run into each other and then they hit each other and then one falls down and that's it. I remember we were fighting them to get it pushed through, while at the same time they were promoting sniper games and other gun games. And it's like, okay, why are they not getting flagged for violence?*
>
> **Small Business**

> *We can basically put in an appeal when they say you've been disapproved. And sometimes I have to do it again and again, and get on a live chat with a support and say, look, we have the certificate, we're licensed to sell this over-the-counter medication etc. Sometimes we're fully compliant, but they'll still disapprove everything.*
>
> **Small Business**

3.3.2.2 Managing platform settings, features, and tools

Many advertisers felt that platforms were 'pushing' advertisers to use platform-native tools, including AI tools. In large part, this perception came from the platform auto selecting the native tools in the campaign settings. Some advertisers passively accepted or even welcomed the auto-selection of these tools, assuming that their campaign may be prioritised or perform better if they use the platform-native features. However, others found themselves meticulously turning off these tools each time they launched a new campaign, which they often considered to be an irritation and a time sink.



Some platforms (Meta in particular) were noted for making changes to the journey steps or layout without warning advertisers. Advertisers ended up repeatedly needing to re-learn platform idiosyncrasies, including the location of some of these platform-native tools. This could again, feel like a point of minor friction in the set-up journey.

> *'Automatically created assets' is what it's called in [platform]. And I turn that off every time I can see it is enabled or anything's been created for two reasons. Firstly, I like to make sure I have control and know what is being put out there. And secondly, I see some of the text being used violates brand guidelines.*
>
> **Small Business**

> *There seems to be more and more AI creative enhancements turned on every single day… At an agency which, working with such big clients as we are, it's a no for us to have any of those turned on. But it has slipped through the net a couple of times and it's just so easy for things to slip through the net because they're releasing new features and we are not aware of them without having to click through every single option and then having to like realise ourselves, oh, this is new, it's automatically turned on and it shouldn't be.*
>
> **Media Agency**

3.3.3 The role of AI in the advertising pathway

As mentioned earlier, during the campaign set-up journey, advertisers often sought ways to enable ease of use and efficiency. AI tools were felt to increasingly support this, primarily when creating ads and optimising performance. Most advertisers also suspected AI to be used by platforms 'in the background', such as in their targeting algorithms and review processes.

3.3.3.1 Types of AI used

The two most common ways advertisers reported interacting with AI were:

1. Generating ad copy and creatives
2. Optimising performance

AI was also sometimes used during campaign performance reviews, to generate reports and was suspected of playing other background roles such as reviewing, checking, and approving ad content.

Generating ad copy and creatives

Both external third-party tools as well as platform-native tools were said to support advertisers in designing ad copy and in the overall creative development.

External third-party tools, such as ChatGPT and Canva were sometimes used to help write and define captions, hashtags, and keywords. Canva and Nano Banana Pro were seen as useful for generating and auto-editing images/backgrounds. Higgsfield and VO3 AI were used to create videos, including adding AI voiceovers where necessary.

Native tools differed by platform and could offer site-specific benefits. Advertisers reported that Meta offers tools that generate multiple ads from a single image, suggesting music and tags, allowing flexible use of creatives and text for optimal targeting, often merging elements of successful ads into another execution from the same advertiser. Google Ads was said to use an advertiser's company website and information to generate and/or edit ad creatives. One advertiser said Amazon generates description and creates 'lifestyle' shots using a product image.

> *I mostly use ChatGPT for ad copy, especially on Meta. I particularly like some of the copy it gives me. But sometimes I have to change a couple of things. I don't think it's 100% built and ready to go.*
>
> **Medium Business**

> *You just set the budget, set the tracking up and then just click publish. Within about 5 minutes I can have an ad with 100 different variations. It's a nice simple tool. AI, definitely in the last few months, has helped massively.*
>
> **Medium Business**

Optimising performance

For optimising performance, external tools, such as ChatGPT and Gemini were sometimes used by advertisers to decide on and refine their overall campaign strategies. Pixis was also referenced as a tool that connected ad manager sites with an advertisers' social channels to automate budgeting decisions, for example, increasing spend on common paydays (such as the end of the month) when customers may be more willing to spend money.

Meta was said to offer two popular site-specific tools to optimise targeting and overall campaign performance, Advantage+ and Lookalike Audiences. Advantage+ could refine targeting, find audiences, and optimise ad placement. Lookalike Audiences would use data to find and target similar audiences and customers in the database. Some advertisers also mentioned Google's App Campaign**,** which could automate and optimise ad delivery to relevant audiences and across Google platforms.

Campaign performance reviews

When it came to reporting on the performance of the ad, external tools such as Ad Spot Dashboard were used by several advertisers to consolidate data from across different platforms and sources and share real-time metrics. Native tools, such as on Google Ads, Meta, and TikTok, were said to have auto-generated campaign reports, which most assume were generated using AI.

> *A Google Ads campaign will build an audience based on its machine learning and smart bidding, which it [the platform] thinks will match the people most likely to convert to that goal. So, what you do is, you run it for [around] three weeks, spend [a recommended budget], and then you'll get past the 'learning phase,' after which it [the algorithm] really starts to optimise performance.*
>
> *You can end up getting lots of people who install the app but don't do anything after. And you can't really blame the algorithm for that, because that's what you've told it to do [i.e. optimise for installs rather than deeper engagement].*
>
> **Large Business**

> *There's an AI element across all these ad platforms in some way, shape or form which tells you things like 'this particular campaign is seeing this much percentage of higher whatever your target was.*
>
> **Large Business**

3.3.3.2 Perceived benefits and drawbacks of AI in the online advertising pathway

Overall, advertisers saw many benefits to the integration of AI into the online advertising journey, saving time and optimising the campaign at a scale and pace not possible before. Perceived benefits included:

- Efficiency: for those who liked the platforms' native tools, AI offered strong time saving and efficiency benefits as advertisers could enable automation of complex functions and skills such as targeting.
- Lower barrier to entry: AI tools were perceived to make it easier for less confident or experienced advertisers to run successful campaigns. For example, the ability to create a polished and professional ad 'at the click of a button' without any professionally crafted assets or copywriting.
- Creativity at scale: AI enabled advertisers to generate hundreds of different versions of an ad in minutes, saving time and creative agency costs, particularly for smaller businesses with limited resource.
- 'Live optimisation': AI can compare different versions of the campaign creatives against each other in real time, to determine the optimal combination to show audiences and adjust content based on incoming data.

That said, there were also some doubts about AI's overall usefulness and capability, including:

- **Lack of transparency in campaign optimisation**: advertisers often felt frustrated by the lack of transparency about how AI campaign optimisation tools (which are typically native to the platform) worked. This could mean that advertisers were unable to access the data to show which ads or combinations of ads performed the 'best', as well as which ones AI was prioritising and why. This made it difficult to take learnings from one campaign to the next.
- **Inefficiency**: in many cases, AI was seen as a 'blunt instrument', making decisions and executing actions on the part of the advertiser and platform without offering explanation as to why it acted in a certain way. For example, the AI could sometimes break targeting objectives and target the wrong audience (ex. targeting women for a male-centred product), or spend large amounts of a campaign budget in short intervals without explanation
- **Poor quality engagement**: some advertisers had doubts as to the quality of engagements their ads received when AI was given control over targeting. These advertisers suspected the algorithm may prioritise overall number over quality (to maximise platform revenue), meaning their ads could not always reach the right audiences and end up wasting budget.
- **Poor quality creatives**: larger businesses, media agencies, and well-known brands often felt AI-generated creatives were flat, inauthentic and unoriginal. Some also felt they often violated brand or regulatory guidelines. Where a platform utilised AI to optimise engagement and generate combinations of text and creatives behind the scenes, the lack of transparency could make it challenging for an advertiser to know if or when this may be happening. For example, by not including a mandatory risk disclosure sentence in an ad for a financial product.
- **Less secure**: a few advertisers made a connection between AI tools and the ability of fraudulent actors to quickly generate professional looking ads without any professional input, though no advertisers had experience of this in reality.

> *We've recently brought on a third party who helps us. They're called Pixis. They help us to use AI tools to somewhat help with optimisation and performance. And it has actually been working for us.*
>
> **Large Business**

> *It's easier to use the AI tools, especially what Facebook have been developing themselves over the last few years, or even 3-6 months. It's so advanced.*
>
> **Medium Business**

> *When designing the audiences to target, I avoid Meta's Advantage+ AI Audiences – I have found repeatedly clients who have wanted to target a particular gender or age or geography have had money wasted by the AI showing the ads to people outside of the set audiences.*
>
> **Media Agency**

3.3.4 Boosting content

Boosted content was defined in this research as content which looks like a user's post, but where the user might have paid the service, so it is 'boosted' or 'promoted' more widely beyond their followers.

Advertisers reported similar experiences when boosting content as when posting or duplicating original ads, with the same checks and reviews in place. Platforms were reported as using different terms or titles for this type of content, such as LinkedIn's '*thought leadership ad'* or '*boosting'*, whilst YouTube and TikTok referred to them as '*promoted'*.

Advertisers felt that boosted content worked best for amplifying content or a strategy that already proved it was working, capitalising on the success of existing posts and/or customer/client reviews, including influencer posts. It felt easy, accessible and low-cost, with no additional or 'professional' creatives needed. Boosted content was also felt to deepen engagement with a trusted community and drive better quality engagement as it may look less like an ad and therefore feel more genuine in the context of certain social media brands where advertisers felt it was difficult to capture customer attention and where customers often scroll-past ad content, such as on LinkedIn and TikTok.

The overall flow of creating boosted content was felt to be very similar to launching a 'regular' online ad. Advertisers could either go to the organic content to boost it or go to set up a new ad and browse existing content to boost. They would then need to define targeting and budget and they perceived there to be a 'review' stage by the platform, in the same way other types of ads are reviewed before they go live.

Overall, the safety and security measures to protect against fraudulent advertisers felt similar for boosted content as it did for display and search ads given the similar set-up and launching processes.

> *They're [boosted ads] often one of the best performing ads because it looks like a regular post in your feed. There's just a tiny thing under their name that says, 'promoted by' and then the company name.*
>
> **Small Business**

> *When we're pushing creator spend, we're also pushing the agency as well because they get some money from that. When you work with creators they can post things organically so they can just post it on their own page and then we can put paid spend behind it and then we can add that into our campaigns with our regular setup dark ads [social media ads which are only visible to the specific audience they are targeting] as well.*
>
> **Media Agency**

3.3.5 Business vs personal accounts

For many platforms – particularly social media platforms – individuals in the business already held personal social accounts with the platform (for example, Instagram or Facebook accounts). These businesses reported having the option of setting up a business account or letting their employees access the company account to advertise via a linked, personal account.

Most advertisers, especially those in larger businesses or media agencies, used a business account and felt this was increasingly becoming the norm. Some of these businesses referenced internal policies and procedures requiring them to have a business account as part of their wider data and General Data Protection Regulation (GDPR) requirements.

Business accounts were also perceived to carry some additional benefits compared to personal accounts, for example:

- Centralised tracking and management of campaigns with ability to grant access to multiple employees for more oversight on activity on the platform.
- Easier management of access as assigned admin accounts could remotely remove employees who were no longer working at the organisation. While advertisers tended to think about this as a benefit for managing the account, some recognised that this could also be an effective tool to prevent account takeover, i.e. unauthorised users gaining access.
- Additional layers or checks before campaigns go live, for example some advertisers reported that business accounts could alert an assigned employee before a campaign goes live who then must approve and confirm that it is ok to be posted. This felt primarily useful in terms of checking campaign content before it went live, but some recognised that it could also help protect against account takeover and fraudulent actors posting ad content via the account.
- Improved customer service and, depending on spend, access to an account manager.

Some advertisers also reported a feeling that there was a wider societal shift toward strengthened online security and felt having a business account, mandated 2-FA logins and dedicated internal policies came as part of that shift. Media agencies in particular, mentioned that they were required by the platform to work via business accounts given they were acting on behalf of multiple clients.

> *I'm using a business account. It makes sense because of the whole GDPR thing, you know. If you leave the business, your access will be revoked. If you've got a private account, you might still have access after you leave. I think it's a security thing.*
>
> **Large Business**

> *We moved over to business accounts last year. It's now a company rule to have a business account because it adds a level of security. It stops risks like hacking into personal emails. It's all linked to your work email address and two factor authentication.*
>
> **Large Business**

Micro businesses and sole traders more often reported having a personal account as they felt this would be sufficient for their purposes and require less nuisance when setting up the account. These advertisers did not mention or reference any potential security downsides to holding a personal rather than business account.

> *As a customer or as an outsider, even if you're looking at our pages, you're not going to know that [our business Facebook account] is connected to my personal account… But maybe further down the line, if we expand and we're a much bigger company, I think we will need to look into creating a completely separate Facebook account that's not a personal account.*
>
> **Micro Business**

4 Perceptions of safety and security

4.1 Section overview

This section explores advertisers' perceptions of the overall safety and security of the online advertising ecosystem, including experiences of and views on safety and security measures they encountered on different ad platforms. The section details reported safety measures experienced at each stage of the ad journey, and how experiences or perceptions differed by business size and industry.

4.2 Spontaneous perceptions of platform safety and security

Unpicking the perceived safety and security of ad platforms from actual or experienced measures was challenging. Advertisers' understanding and impression of platform safety was often based on multiple influences from both inside and outside of their professional experience, including anecdotes and historical narratives, rather than technical reality. The gap between perception and infrastructural reality is fundamental to understanding advertiser confidence in platform safety and security.

The following sections explore this in more detail with Sections 4.2.1 and 4.2.3 explaining the perceptions, and Section 4.3 explaining the reported experiences.

4.2.1 What drives perceptions of platform safety

Perceptions of platform safety tended to centre around three core elements or experiences:

1. Advertiser experiences as a consumer

Advertisers are not just engaging with platforms and sites in their professional life, but they are also regularly using many of the sites they advertise on, as consumers. Their perceptions as consumers significantly shaped their perceptions of ad platforms from a professional sense.

This encompassed the types of ads they encountered on a given platform, the overall quality and relevance of the ads they noticed on the platforms, and the composition of platform users or audiences. Advertisers developed greater confidence in a platform's safety mechanisms when they noticed high-quality ads, aligned with their interests. Conversely, where they noticed irrelevant, low-quality or potentially fraudulent ads when browsing as a consumer, their trust in the platform as an advertiser was undermined.

Additionally, the platform's userbase influenced perceptions, in terms of whether it could be considered trustworthy or reputable. This could include both perceived risk of bot interactions, as well as the platform's role within broader digital discourse; particularly whether it was associated with more polarising or sensitive content areas (e.g. politics). Advertisers generally felt that platforms perceived to host highly engaged and contextually relevant audiences felt more aligned with brand safety objectives than those where content quality and tone were seen as more variable.

> *We do see a lot on Facebook. [Ads that are] clearly set up to make people think it is a charity appeal kind of thing. You know, the 'sad old man without any heating' imagery, and it's a stock image or it's an AI-generated image. And they're either boosting the post or they're just using bots to try and push the message.*
>
> **Medium Business**

> *It's like I saw around the other day on TikTok that was. It's like this Star Wars spaceship and it was like, you know, 29.99. And I thought that seems ridiculously low and looked. And this is something that retails for £500 on Lego. So clearly this is going to be a fake that obviously kind of got through.*
>
> **Medium Business**

2. Brand reputation

Platform brand reputation served as a powerful proxy for safety perceptions. Advertisers often projected a platforms' broader brand values and historical positioning onto safety assumptions. A platform with a strong reputation for user protection and brand safety tended to benefit from positive spillover effects. Where platforms have experienced publicised brand controversies, advertisers were more sceptical about the robustness of their safety measures, regardless of actual systems in place.

Additionally, platform brands perceived as having values aligned with mainstream users were perceived as having tighter content controls, whereas 'brands' perceived as hosting (and encouraging) more niche, or potentially controversial communities faced suspicion about ad quality and platform safety standards.

> *People just don't trust the platform [X] as much anymore. And maybe this news about Grok these past few days has really made that a harder or an easier decision for people to walk away then.*
>
> **Media Agency**

> *But I would say TikTok Shop…Or TikTok, is probably the worst for it… they sell a lot of things that just don't make sense. Like I've seen that they sell like rotisserie chickens. I'm like, why? How can you be selling hot food? It doesn't make sense.*
>
> **Media Agency**

3. Platform infrastructure

Platform infrastructure, defined, for the purposes of this research, as the technical systems and policies governing ad placement and content moderation, ostensibly determines actual safety outcomes, but perceptions of these systems were themselves also crucial.

The sophistication of a platforms' targeting capabilities was a particularly important but complex driver of perceptions. For some advertisers, more advanced targeting algorithms were associated with potentially more robust security, as they assumed the platform would generally have greater technological sophistication across the board. However, other advertisers interpreted the same targeting capabilities as a potential way in which ads could be misplaced (for example, placing ads on sites the advertiser would not want to be associated with) or audiences manipulated (for example, by enabling non-specialist or illegitimate actors to advertise fraudulent products efficiently and effectively).

Data quality and impression authenticity also shaped perceptions. Platforms perceived as delivering impressions from genuine users with reliable engagement metrics were felt to hold stronger safety credentials than those suspected of generating artificial or low-quality impressions. This was compounded by the transparency of impressions data. Where platforms were perceived to be more secretive or opaque

with the data, advertisers could presume this was to 'hide' low-quality and therefore may take a similar approach to overall platform safety.

> *One thing is, which was very annoying even in Meta, for example, it'll randomly say that oh, these many likes have happened, or this is the click through ratio or oh, the website traffic has been XYZ numbers. But when you actually check the site traffic or even the posts' likes for that matter, sometimes you'll see that the data is very inconsistent.*
>
> **Micro Business**

Frequency and transparency of ad reviews also influenced advertiser trust in platforms. Platforms that were felt to visibly reject large volumes of ads, particularly those demonstrating proactive moderation of ads, were perceived as maintaining stricter safety standards across the board. Conversely, platforms with less visible or less frequent ad rejection processes were assumed to be less stringent with their controls, even where this perception may not reflect the reality.

> *They're all a bit pants. They kind of give you like a generic category for why it's been blocked. So you'll get like Facebook, it'll be like, oh, this has been flagged for like social causes, political, or this has been flagged for like employment or the special categories that they have. But it doesn't specify where the issue is. It doesn't specify if it's the graphic, if it's the wording, if it's the URL. Like, you can be flagged up on the URL.*
>
> **Medium Business**

Overall, consumer experiences, brand reputation and platform infrastructure were deeply interconnected when influencing advertiser perceptions.

4.2.2 Overall perceptions of platform safety

Overall, advertisers started from the assumption that most, if not all, advertising platforms (open web or walled garden) would have a policy in place, outlining what can and cannot be advertised, and what can and cannot be included in ads themselves.

However, most advertisers had not engaged with the detailed policy itself, primarily because:

- They did not feel they had any need to when they first opened the account.
- In the case of ad rejections, they were unsure where in the policy they would find relevant information.
- They considered the process of engaging with the policy time-consuming.

In some cases, ads had been rejected and the platform had flagged them for breaching certain rules or a certain policy, however, advertisers often found it hard to understand what the issue was. The wording used to explain the reason for rejection often felt vague and non-specific. This felt especially true when a video ad was rejected as advertisers felt platforms rarely, if ever, explained what part of the video was in breach of the rules or policy leaving them to question if it was the music, voice over, text on screen, imagery and so on. Taken together, this could make it challenging for them to correct for the issue.

Beyond the baseline policy, the factors mentioned in Section 4.2.1 above heavily influence perceived safety, especially in relation to more well-known platforms and brands. Detailed findings about how advertisers tended to categorise different well-known brands can be found below.

More safe and secure

LinkedIn: The professional nature of LinkedIn profiles and content creates a 'halo effect' around the platform, building a perception that the platform would have more stringent and reliable checks. For some advertisers, this was supported by experiencing moderately frequent rejections of their ads, suggesting the platform was conducting sufficient reviews.

Google Ads: Advertisers tended to feel Google Ads was one of the most 'strict' and proactive when it came to fraud prevention. This tended to be linked to Google Ads' infrastructure, including sophisticated targeting and frequent reviews and rejection of ads, as well as email alerts when new users logged in and rulebooks or policies related to regulated products or services such as health and financial services. Advertisers felt Google Ads took regulatory compliance seriously.

> *I feel like LinkedIn is one of the better advertising platforms for security. I don't have many concerns with security by LinkedIn.*
>
> **Large Business**

> *I think Google I feel quite safe with because as much as I find them annoying at points, they are meticulous in what they do. And, you know, like the fact is, like, they'll always email you, they'll always be like, right, do you need this? Like, they've got so much information online that's readily available to you.*
>
> **Medium Business**

Somewhat safe and secure

Meta: While some advertisers appreciated the sophisticated technology on Meta (e.g. targeting tools) which could imply more advanced safety and security monitoring, others reported regularly witnessing copycat sellers, fake accounts and scams on the site (e.g. fake music event pages selling false tickets to fans), leading them to doubt the overall security.

YouTube: There was some sense that YouTube benefitted from the safety and security of the Google ecosystem. However, several advertisers reported negative experiences as a consumer impacting their professional perceptions of the platform safety and security. These advertisers mentioned seeing frequent consumer-facing scam ads on YouTube itself, often using fake images of famous YouTube stars. This was felt to undermine trust.

TikTok: TikTok provoked mixed reactions when it came to overall perceived safety and security. A number of advertisers pointed to the platform infrastructure as an example of strong safety and security. These advertisers had experienced relatively frequent rejections of their ads due to (what sometimes felt like over-precautious) flagging of imagery and content for going against 'community guidelines.' These advertisers felt the frequency of these types of checks signalled TikTok was strict on safety and security. Likewise, a number of advertisers felt TikTok had more stringent rules restricting advertising certain types of healthcare or medical products.

However, others pointed to their experiences as a consumer as well as professional experiences of TikTok shop as a signal that TikTok was not safe or secure against fraudulent ads. These advertisers felt that they often witnessed ads that felt like 'scams', had seen their own merchandise being sold second-

hand (illegally) on TikTok shop, and some also had heard stories about TikTok Shop vendors copying the branding of larger brands whilst selling low-quality or 'fake' goods. TikTok shop was generally perceived as less secure, which could influence perceptions of TikTok overall.

> *One example I can give is giveaway scams using the face of… a popular YouTube figure. They say 'click this link and you'll win £200'. It's just blatant false advertising. I see those things on YouTube a lot more than I see on Meta.*
>
> **Medium Business**

> *I would say that TikTok shop is a bit of a jungle at the moment. I think they definitely need to tighten it.*
>
> **Medium Business**

Less safe and secure:

X (formerly, Twitter) was most consistently perceived as the least safe and secure platform. These perceptions tended to come from a combination of the platform's brand reputation and consumer experiences of the brand. Advertisers mentioned that the recent re-branding from 'Twitter' to 'X' came with a change of brand direction, and potentially brand values. Some actively avoided advertising on X as they felt misaligned to the platform values and did not want their brand associated with the platform. In combination with advertisers reporting more prominent 'scam' ads on the platform when browsing as a consumer, advertisers felt the platform was potentially less safe and secure than others.

> *Twitter… seems to attract more trouble than it's worth. So, we haven't even tried to verify there.*
>
> **Media Agency**

4.3 Experiences of safety and security measures in the advertising journey

At an overall level, advertisers perceived ad platforms as prioritising revenue generation over all else, including fraud prevention. Investing in or enforcing effective safety and security measures felt like a secondary motivation and at its most extreme, a 'tick box' exercise rather than meaningful action.

Advertisers pointed to two key 'evidence' points to support this view:

1. **Platform transparency and structural incentives:** The structural dynamics of the perceived most dominant platforms (primarily Google Ads and Meta) reinforce advertiser scepticism about platform intent and priorities. Advertisers perceived Google and Meta as monopolistic entities with growth and revenue maximisation as their primary organisational objectives. This perception was felt to translate into observable behaviour. For example, advertisers with higher spending levels were perceived as receiving closer, more responsive support, implying that account priority correlates with revenue potential rather than risk profile or security needs.

   More fundamentally, platforms (especially Google Ads and Meta) were seen to be operating as "black boxes" from the advertiser perspective. Both platforms' targeting algorithms remained protected and

inaccessible; advertisers stated that they were unable to view comprehensive data on impression quality, engagement authenticity, or audience composition. This perceived opacity creates scepticism about whether platforms are genuinely monitoring safety or protecting business models from external scrutiny. The implicit message advertisers receive is that platforms will only respond to security concerns when compelled to do so, for example by regulatory pressure, rather than proactively prioritising fraud prevention as a core operational principle.

> *They all work as a black box. So, you know, you put in what they require and then they spit out results. But in between, then you have no idea what's going on. I think some level of transparency would be great to know*
>
> **Small Business**

2. **The type and depth of issues or content being screened for**: Advertisers reported that the categories of issues platforms tended to flag as problematic were often narrowly focused, signalling a desire to be compliant but not necessarily implementing wide-scale prevention of fraudulent ads.

   Most ad rejections that advertisers reported experiencing related to aesthetic or surface-level issues for example, background and text colour clashing, large chunks of text, and design inconsistencies. This was coupled with relatively easy workarounds, for example, when ads were rejected for cosmetic reasons, advertisers reported altering punctuation or removing and re-adding words**,** which once re-submitted, tended to be approved and go live without issue. The ease of workaround was felt to suggest platforms are not conducting meaningful checks into why content was flagged but rather are implementing automated and surface-level checks.

   While some advertisers referenced certain platforms, such as Google Ads, as being more active in flagging regulatory concerns (e.g. ads for cryptocurrency products in financial services), most felt these types of issues represented a minority of ad review and rejections. As a result, advertisers often felt this pointed to performative action than genuine and meaningful attempts to reduce or prevent fraudulent activity.

> *On Google, we've been rejected for imagery, not because there was anything wrong with the imagery, just because Google doesn't like text on top of images. So that's always a fun one. And it also doesn't like it if you have exclamation marks where it doesn't feel it's grammatically correct. And it is one of the most intricately nitpicky systems I've ever met in my life.*
>
> **Medium Business**

All that being said, advertisers did report the presence of multiple safety and security measures and policies throughout the online ad pathway, including at account set up, when managing their account day to day, when they set the campaign to live, and when advertising in certain industries. Sections 4.3.1, 4.3.2 and 4.3.3 outline the reported safety and security measures in further detail.

4.3.1 Account set up

It is important to note that findings related to account set up processes are based primarily on advertisers' memory. They were often recalling setting up an account from several months to several years ago and as such, some of the detail in the process may no longer be accurate.

Advertisers reported that when using a business account, platforms require baseline verification during the creation and set up of an account. Verification tended to be about providing a range of documentation and information to confirm the business existed and was legitimate.

Standard requirements across platforms typically meant providing:

- Links to the company website, or social media page (e.g. company Instagram or Facebook page)
- Corporate registration documentation or proof (e.g. VAT number)
- Payment method verification, usually small test charges when setting up the account details
- Self-declaration of the product/service category (e.g. political, financial, charity)
- Identity documents such as passports, drivers licences or utility bills

> *At the start, there would have been verification checks on the business owners, and we obviously had to provide the registration number for the company.*
>
> **Small Business**

However, advertisers were sceptical about how substantial or meaningful set up checks and verification was. Many questioned whether these requirements were genuine safeguards against fraudulent actors, or more of a formality that creates the appearance of verification without scrutiny. Several factors fed into this scepticism, including:

- **Speed of review**: advertisers reported some documentation reviews as incredibly quick, suggesting that the review was likely automated and not very thorough. TikTok was mentioned as a particular example here with advertisers reporting reviews taking around 25 minutes.
- **Depth of verification:** advertisers widely assumed that URLs, VAT numbers and corporate documentation could easily be fabricated or misrepresented (e.g. a fraudulent actor could provide a link to any Instagram page), and it is unlikely that a platform would flag this as an issue. Advertisers doubted platforms were cross-checking any information provided.
- **Absence of ongoing verification:** once an account is approved on a platform, advertisers reported that they were not required to re-verify at any point. Advertisers stated that accounts will go unchecked unless specifically flagged for violating platform policies.
- **Focus on payment functionality:** Payment detail verification was perceived as the most rigorous check, by which advertisers referred to ensuring credit cards, bank accounts and other payment methods worked. The focus on payment processing rather than advertiser legitimacy reinforced a perception that platforms prioritise revenue over fraud prevention.

> *When you're first doing it on an ad platform that you've never used before, they tend to take a day or two or a handful of days before things actually go live. But the more you use the account, the more that trust is built and they go live quite quickly*
>
> **Medium Business**

Beyond the ‘standard’ account set up requirements, advertisers also reported some platforms offering optional ‘verified status’ which triggered additional safety and verification layers. Meta’s Facebook “Blue Tick verification was the main example provided. Advertisers recalled needing to submit additional documentation beyond the standard required for onboarding, including additional identity and financial documents (utility bills, bank statements, VAT certificates). Whilst advertisers who had been through this

process praised the additional layers of security, they queried why this was not the standard approach for all businesses advertising on the platform.

> *Facebook, if you want to have a Blue Tick verification, you have to supply some documents and some of these documents might include your bank documents or the address of the business… I don't believe they do that when you actually create an account. I think they only do that for the bluetick verification, which I find really strange.*
>
> **Large business**

4.3.2 Day to day account management

4.3.2.1 Logging in

The most commonly experienced daily security measure experienced across advertisers was multi-factor authentication (MFA). Advertisers were often triggered to complete MFA every time they logged into their account. Some also reported having to complete MFA just before setting a campaign to go live (e.g. on Google Ads). Advertisers reported completing MFA across platforms and environments including both walled-garden and open-web platforms and felt that overall, it was an effective preventative measure for account takeover. Whilst MFA introduces a moment of friction in the journey, advertisers felt it was an important step to assure on security and so it was perceived as an acceptable disruption.

MFA was widely accepted as a standard expectation when managing any digital account, not just in online advertising. Advertisers reported using MFA on personal accounts, as well as other work-related systems or accounts (e.g. when logging into work email). Whilst advertisers were not often clear on whether platforms required users to have MFA set up, most felt it was an expected best practice approach.

That said, a small number of advertisers reported different experiences of MFA depending on whether they had a personal or business account with the platform. One advertiser explained that the company used to allow employees to use personal accounts connected into the organisation page. When this was the case, they were regularly (multiple times a day), automatically logged out of their account and prompted to log back in using MFA. Whilst the advertiser appreciated that this may have been to ensure the account was secure, the frequency caused significant disruption to the workflow. Since moving to a business account due to the company's strengthened security policies, the advertiser is only prompted to complete MFA when logging in.

Beyond MFA, several advertisers raised that they had experienced Google Ads in particular, sending emails directly to admins on the Ad Manager account when new devices logged in. This enabled advertisers to review and remove unauthorised users if required.

> *On Meta, we have a six-digit code that gets sent to me whenever I log into it. I have two-factor set up on LinkedIn too.*
>
> **Small Business**

4.3.2.2 Making changes to account settings

A proportion of advertisers reported security checks when attempting to make material changes to business account settings. The type of change or event that typically triggered a check included:

- Adding new users or team members to the account
- Editing administrative access or user permissions

- Changing banking or payment details
- Materially increasing advertising budget

When these changes occurred, advertisers reported platforms such as Meta Ads Manager prompting additional checks, such as:

- The platform will send an email notification to the individuals named as the account holders (e.g. finance managers, company directors), prompting them to explicitly approve the change or provide a verification code
- MFA is triggered which the individual has to complete before they can finalise the change
- Temporary account locks until authorisation or MFA is completed

Advertisers generally felt these checks were meaningful, as they require intervention from an independent or approved colleague, and there was a sense that they cannot be easily worked around.

> *I think 2FA is a good step. I was on Google early today and if I want to increase the budget by a certain amount for example, I will need to verify for that increase.*
>
> **Large Business**

4.3.2.3 Posting an ad

Most advertisers reported a delay before an ad went live across platforms, and most had also experienced an ad being rejected. Some advertisers connected these delays and rejections to platforms' safety and security measures. For example, they perceived that if an advertiser was newer to a platform, they are likely to have a longer delay which they presumed was due to the platform needing to check their content and business were legitimate.

Likewise, some advertisers experienced ads being rejected due to, what the platform saw as, regulatory conditions being breached. This was particularly true of those in financial services and/or gambling where they felt platforms (especially Google ads), were particularly stringent in reviewing and rejecting ads, and this could mean illegitimate or potentially fraudulent actors would be more likely to be picked up if trying to scam consumers within these industries.

> *The campaign will go live in maybe 15 or 10 minutes. Maybe sometimes longer. It can take up to an hour.*
>
> **Medium Business**

> *The things we've been rejected for tend to be where we've been overly cautious with our disclaimers. How prominent our disclaimers are to the detriment of what Google will call 'creative quality'. We've also had stuff rejected in the past where, for example we launched a product related to the US and [the image in the ad] had a US flag and… the [US city] skyline. I think that ad got rejected for being political or something.*
>
> **Large Business**

That said, as mentioned in Section 4.2, many advertisers doubted whether there was a meaningful connection between campaign reviews, rejections and platform intentions to prevent fraud - as reviews could feel surface-level and more focused on aesthetic issues than the content itself.

4.3.3 Industry-specific safety and security measures

There was a perception that safety and security checks were not uniformly applied across categories or industries. Even for industries that were perceived to be higher-risk or more highly regulated including financial services, healthcare, politics and charities, amongst the advertisers involved in this research, there was a sense that there were inconsistencies in terms of how platforms verified and monitored ad content in these sectors. The existence and stringency of these additional measures were felt to vary by ad platform.

Advertisers reported that it was down to the advertiser to self-declare if they were advertising products in the sectors mentioned above, either during set up of the account or when launching campaigns.

Some advertisers presumed that if an advertiser did not declare they were advertising products in these sectors, the platform would likely pick up on this during its reviews of ad content and flag or block the content. However, this view was based off a perception, and advertisers could not point to direct evidence or personal experiences of this.

Advertisers working in these spaces often had some broader awareness or understanding about what they could or could not say in advertising built out of their experience in the sector, rather than engaging with policies on the platform itself.

Financial services and healthcare or medical advertising prompted the most detailed discussions during this research amongst advertisers. The following sections explore each of these sectors in detail.

4.3.3.1 Financial Services

Financial services advertising was perceived by some to entail the most rigorous verification requirements, particularly on Google Ads, where regulatory oversight and advertiser legitimacy concerns were felt to drive more intensive checks.

Google Ads' approach was felt to represent the highest standard of industry-specific verification. Advertisers in the financial services sector reported needing to go through mandatory verification demonstrating Financial Conduct Authority (FCA) status and providing evidence of a named representative to confirm this. These advertisers reported the process extending over several weeks and that it was required before they were able to advertise on the platform. In these cases, advertisers believed Google Ads was conducting substantive background checks and that if an advertiser failed to declare their status or attempted to advertise financial services or products from an unverified account, Google Ads would detect the activity and block it. There was confidence that Google Ads was proactively monitoring and acting on this industry.

> *They required financial services verification. And what that meant for us was providing evidence of our FCA regulation, providing evidence that we did not sell cryptocurrency or that we were not a cryptocurrency thing.*
>
> **Large Business**

Meta's approach was felt to be less consistent. Some advertisers reported requirements similar to Google Ads' (mandatory self-declaration, submission of FCA evidence), whilst others reported that self-declaration alone was sufficient. There were therefore questions around the process and rigour in these instances.

4.3.3.2 Healthcare and Medical Advertising

Much like financial services, healthcare and medical advertising cover a similarly sensitive regulatory space, triggering platforms to implement additional or different safety and security checks.

Google Ads was specifically referenced as enforcing healthcare-specific requirements and advertisers also mentioned the platform had detailed content policies, specifying what types of claim were permitted or not in health-related advertising. Advertising containing content of this nature was also perceived to be subject to more frequent reviews, pausing, or flagging on the platform. For example, advertisers spoke about Google flagging and rejecting ads that mentioned 'prescription medication' or where an advertiser may try to target specific individuals based on characteristics that feel related to health (for example, targeting someone with an ad that says 'we know you're struggling with hair loss. Here is a product for you').

> *Google has a very long detailed list of the sort of thing you can and can't say by industry. Often things get flagged for mentioning words such as 'prescription medication'. It will flag it, say we need to change it and pause the ad. Sometimes it's just for medical products generally. I probably get disapproved once a week with Google.*
>
> **Small Business**

By comparison, Meta was felt to take a less proactive approach. However, a small number of advertisers perceived that Meta had become increasingly strict on stopping ads that claimed or implied specific health outcomes, which some advertisers thought could typically be associated with 'scams' (e.g. weight loss 'miracles').

Some advertisers felt that TikTok implemented some of the most restrictive rules in this area, believing the platform had imposed an outright ban on businesses advertising medical tests and that any ads containing health-related content were subject to stricter moderation and more intensive, potentially manual, review processes.

> *I hear stories a lot that Meta doesn't like the weight comparison ads like the 'before and after' style. They don't like you to get too specific.*
>
> **Medium Business**

> *On TikTok, we can't advertise our product because TikTok don't let you advertise any medical tests whatsoever.*
>
> **Small Business**

4.4 Experiences across business types and sizes

Larger businesses, and media agencies, reported greater internal focus on safety and security more generally, which then extended to security of online advertising accounts. Whereas microbusinesses, sole traders and those outsourcing paid advertising to an external agency reported less interest and focus on maintaining safety and security.

4.4.1 Larger businesses and media agencies

Larger businesses and media agencies were often supplementing the platforms' safety and security checks with their own internal processes as part of their wider organisational online security policies and procedures. These internal processes, as outlined below, were felt to provide an additional layer

of assurance against potentially fraudulent activity against them as organisations, particularly account takeover.

1. **Third-party tools and services**. Some larger businesses and media agencies had partnered with external, third parties which introduced an additional step in the process before an ad campaign was able to go live or changes are able to be made to the account. For example, one advertiser was using a third-party tool called AutoQA which they explained as connecting into their systems and triggering an approved colleague (e.g. a Director) to review and approve any campaign before it is able to go live.

> *Someone logged into our Ads Manager and tried to set religious content live in one on our clients' Ad Managers. We work with a programme called Auto QA, that means we have to go into different websites and account managers have to approve campaigns; we have to get two approvers. This means the campaign couldn't go live. The hacker wasn't able to spend the money they wanted to.*
>
> **Media Agency**

2. **Internal review processes and procedures.** Some larger businesses and media agencies explained that their company had processes in place to ensure there were several layers of approval and checks before any campaign went live. This could include creating reviews, brand guideline checks, compliance checks and approvals. Whilst not directly preventing fraudulent activity on the account advertisers felt the processes made them feel safer and more secure.

> *All our words, our creatives, must be approved internally by brand teams. And by compliance. There is that other, sort of, shield.*
>
> **Large business**

3. **Account requirements**. Most larger businesses and media agencies reported policies and/or a shared understanding within the organisation requiring them to have a business, rather than personal, account as well as requiring MFA to be enabled on all accounts (on ad platforms and elsewhere). See Section 3.3.5. for more detail on perceived benefits of business accounts.

> *When you add someone to the account, another admin has to approve it just so that there's an extra layer of security.*
>
> **Large business**

4.4.2 Smaller businesses and those outsourcing to external ad agencies

Smaller businesses, including sole traders, as well as businesses outsourcing to external agencies often felt they were juggling a wide variety of tasks, with prevention of fraudulent advertising lower down on the priority list. There was some indication of over-confidence, whether that be in the platforms themselves (i.e. they will be sufficiently monitoring for fraudulent advertising already), or in ad agencies especially when thinking about those outsourcing management of paid media campaigns. This context leads to a tension when it comes to perceived need and impact of future prevention of fraudulent advertising:

On the one hand, these businesses may be more exposed to account takeover and brand impersonation on paper, even if this was not something they expressed directly, due to:

- Fewer company-level protections and procedures: these businesses often cited less formalised processes and policies in terms of data security more broadly, especially the smallest businesses.
- Lack of resource and capacity to review, check and manage issues as they arise, and potential lack of specific skill set or expertise to identify potential risk areas. Those outsourcing to external agencies were often doing so due to a lack of internal resource and expertise, so felt they must put their trust in the agency executing their ad strategy to maintain safety and security standards on their behalf.
- Fewer direct routes to contact the platform, as most are not spending enough to hit the threshold that means they are provided with an Account Manager, making it harder to get hold of a 'human' if something goes wrong.

On the other hand, these types of businesses may be less open to the introduction of additional or alternative safety and security measures as they could be disproportionately impacted by any measures that add friction or time to their established workflow. For example, one sole trader used TikTok because it felt very easy and intuitive to set up. If more stringent requirements were required, this may make it hard for similar businesses to set up and start advertising their products or services.

> If you're a one-man-band, or a really small team, you're not really in a position to start from scratch and do all the testing and things.
>
> **Small Business**

5 Experiences of fraudulent advertising

5.1 Overview

This section explores advertisers' perceptions of fraudulent advertising and its impact, alongside their reported experiences of other problematic activity such as 'ad fraud'. The section includes case studies to demonstrate how advertisers responded to fraudulent advertising incidents including experiences of the reporting processes, as well as how platforms addressed issues identified.

5.2 Spontaneous perceptions of fraudulent advertising

As mentioned earlier in this report, safety and security was not generally top-of-mind for advertisers in the campaign process. Prevention of fraudulent advertising fell into this categorisation. Advertisers were primarily focused on achieving their campaign objective at a reasonable cost on a reputable and familiar platform. As a result, there was a sense that for some, the existence of fraudulent ads had become somewhat normalised; an accepted feature of the online ad ecosystem, rather than an issue that needed addressing.

However, when directly explored and/or probed on, advertisers acknowledged that there were potential negative impacts and consequences of fraudulent advertising for them as advertisers, as well as for consumers.

Some advertisers, particularly those in industries that feel potentially more reliant on and sensitive to building consumer 'trust' (e.g. financial services, healthcare), saw a more explicit link between fraudulent ads, the erosion of brand credibility, and therefore damage to consumer trust. For these advertisers, not sufficiently addressing the challenge of fraudulent actors could damage legitimate brands. Consumers may see 'scam' ads alongside legitimate brands and over time, become sceptical of all ads as a mental short-cut to protect themselves from being scammed.

> *If we're serving alongside companies that aren't genuine, that's not a great look, especially in financial services, where trust is a huge thing...I see it quite a lot on Facebook. For example, I saw an ad using images of Martin Lewis [illegitimately]. As an advertiser, even if you know your ads are real, you think, 'is the customer viewing this with the same scepticism as me? Could that have a negative impact [on us]?*
>
> **Large Business**

For other advertisers, the connection was more implicit. Advertisers' decision to avoid platforms perceived to be hosting higher volumes of 'scam' content (such as X, as discussed in Section 3), suggests an implicit recognition of risks associated with fraudulent advertising, particularly in relation to consumer trust, brand integrity and reputational harm.

> *I don't really touch Twitter [X]. They're a bit of a newer platform with new ownership and I think there's still some work needed because every time that I'm on there, most ads feel like a scam.*
>
> **Medium Business**

5.3 Experiences of fraudulent advertising and other problematic advertising activity

Fraudulent advertising was defined in the research as 'scam ads that could mislead customers, for example, a scam or impersonation of a company's brand'.[2] The research sought to differentiate 'fraudulent advertising' from 'ad fraud' (i.e. an internet service or bot creating false interactions like clicks of impressions to generate revenue from an advertiser).

However, it became clear during the research that when advertisers considered the overall safety and security of the online advertising ecosystem, they referenced a broader set of problematic or suspicious activities that extended beyond this formal definition.

In theory, advertisers considered four broad types of problematic activity in the online advertising ecosystem (though individual cases could sometimes fall under multiple types): sharp practice, ad fraud, scams and brand impersonation, and account takeover or 'hacking'. The perceived impact of each of these activities was assessed against two key metrics:

1. Salience, referring to the perceived prevalence of the issue, and extent to which the activity caused disruption to campaign success.
2. How easy or difficult the activity felt to 'police', referring to ability to prevent, prove and monitor.

In practice, the boundaries between fraudulent advertising and other forms of problematic activity within the ecosystem was not always clear for advertisers.

The table below outlines a summary of advertiser perceptions, whilst Sections 5.1.1 to 5.1.4 go into detail about each type of problematic activity.

Type of problematic activity	Perceived salience	Perceived difficulty to 'police'
Ad Fraud	Top of mind and a direct threat to achieving and 'proving' campaign success.	Challenging to prevent and prove and sense of 'powerlessness' against ad platforms.
Sharp Practice (by competitors)	Top of mind and a direct threat to achieving campaign success.	Difficult to prove and low awareness of where to go, and how to report.
Scams and brand impersonation	Relatively common issue and more significant presence on some platforms than others.	Potentially challenging to monitor, but comparatively easier to 'prove'.
Account takeover or 'hacking'	Relatively common, particularly *attempts* to hack; advertisers targeted with phishing emails relatively often, and successful takeovers/hacks were felt to be one of the biggest cyberthreats for businesses.	Easier to manage and prevent via existing measures and mechanisms.

Advertiser perceptions of salience and ease of policing had a direct correlation with their appetite for additional regulation. This is explored further in Section 6.

[2] The definition provided was used specifically to ensure participants understood the difference between fraudulent advertising and ad fraud. The Online Safety Act defines a "fraudulent advertisement" in relation to a Category 1 service, as a paid-for advertisement that amount to one of the Act's prescribed fraud or financial offences, and which is not user-generated content. In relation to a Category 2A service, a "fraudulent advertisement" is defined as a paid for advertisement that amounts to one of the Act's prescribed fraud or financial offences. These legal definitions were **not** used in the research.

It is important to note that the categorisations of ‘sharp practice’ and ‘ad fraud’ explored below are based on advertiser perceptions and experiences and may not always align with formal industry definitions or terminology. Nevertheless, the perceived categories are important as they played a key role in shaping how advertisers perceived and understood the risks within the ecosystem, and therefore, appetite for regulation.

5.3.1 Ad Fraud

Most top of mind when considering problematic activity in the online ad ecosystem was ‘ad fraud’, particularly amongst advertisers who were specifically trained in paid media advertising, and whose job role focused solely on this (more often in media agencies and medium or larger businesses, which tended to have more ‘specialist’ roles). Ad fraud was considered a day-to-day point of frustration that directly threatened their ability to achieve campaign success and prove that to stakeholders.

There was a perception that the perceived most dominant platforms (Meta and Google Ads, as referenced earlier in the report) were intentionally opaque and held the ‘power’ in the relationship with the advertiser (i.e. advertisers could not avoid advertising on these platforms due to their scale). The lack of transparency afforded around engagement data made it challenging for advertisers to verify the quality of engagement data and protect against ‘bots.’

Advertisers spent significant time and effort trying to solve ‘ad fraud’ with some investing in use of third-party products to support, such as:

- Apps Flyer: a ’mobile measurement partner’ that claims to provide more accurate engagement data
- Lunio: a product that claims to help track if a click is a bot, and subsequently block the IP address if it is identified as one

Despite these attempts, most advertisers did not feel there were any fool-proof, fully capable solutions that could unpick ‘ad fraud’ from legitimate engagement, meaning it was an ongoing and unresolved challenge.

MINI CASE STUDY

An advertiser was using an app advertising platform when they saw an article about how the platform was claiming installs and data that was not factual. They went to investigate their own data based off the article and found that the platform had been falsifying engagement, making it appear as though their campaigns were getting better engagement than they were in reality, meaning they were spending more on the platform. The advertiser felt that ‘all these networks’ operated as a “black box” which means it is challenging for advertisers to really know what is going on behind the scenes and therefore protect against ad fraud. This advertiser has started using AppsFlyer as a “source of truth” to reconcile inflated network-reported numbers.

> *All these networks will work as a black box, you put in what they require and they spit out results […] Google will say you spent, I don’t know, $1000 yesterday, you got 100 installs, you’ve got all this other data blah, blah, blah. You can see on AppsFlyer that ok, you spend a $1000 but you actually only got 90 installs and so on. It acts as a source of truth […] whereas networks like Meta, TikTok and Google, they are all what we call ‘self-attributing’.*
>
> **Small business**

5.3.2 Sharp Practice

Sharp practice was also a common and top of mind type of problematic activity in the online ad ecosystem. Many advertisers had experienced what they perceived to be industry 'sharp practice', for example:

- Competitors failing to follow industry standards or regulation
- Brands having similar colours or font to another company, but not directly impersonating a brand
- Companies 'pretending' to have reduced prices to give an impression of a discount
- Whilst these examples were felt to push the boundaries of acceptability, advertisers felt they were less obviously classified as outright fraudulent advertising, and therefore harder to prove and act on.

Advertisers considered the impacts of 'sharp practice' to be direct and considerable not only on their own campaign but also on the wider public. The prevalence of sharp practice was seen as undermining the effectiveness of their own (and others') legitimate campaigns and creating unfair competition. There was also a sense that sharp practice was harder to prove, define, report and resolve given issues were often nuanced, as well as industry or market specific. Advertisers were often unclear on which issues may formally be deemed as fraudulent versus sharp practice, and therefore which types of issues they were able to report via official channels.

A few advertisers considered sharp practice an issue more for advertising and trading standards, rather than prevention of 'fraud' and therefore questioned how far prevention of sharp practice should be a responsibility of the platform itself.

MINI CASE STUDY

One health and wellness advertiser shared a story about a competitor advertising prescription medicine despite industry standards stating that this was not permissible in the UK. This advertiser felt this activity was directly impacting their own company's ability to generate revenue as consumers would not know that the competitor was acting against regulation and would likely purchase from the other brand as a result.

> *The average Joe will see that and think nothing of it and be like, great, they sell [prescription medication], I'll go buy it. Whereas we don't say it and it's obviously meaning we get less sales than them, even though they're technically not being compliant… I think it is having an impact on our business.*
>
> **Small business**

5.3.3 Scams

Whilst not the most top of mind, advertisers were acutely aware of the existence of scams on online platforms, and some, particularly larger or more well-known brands, had personal experiences of brand impersonation. Some of the types of ads that advertisers felt could fall under this category included:

- Fake product listings
- AI generated charity-style appeals
- TikTok 'get paid to watch' offers
- Spoofed websites
- 'Giveaways' for large amounts of money

Some advertisers recognised that presence of scam ads had the potential to erode consumer trust. There was a sense that these ads, even if not related to their own product or service in any way, could cause a wider erosion of trust in online ads, making consumers more reluctant to engage with *any* online advertising and potentially limiting online sales potential.

> *I saw an ad on Instagram... I clicked on the ad... I placed the order... And then when the package came to my house, it was something like, very different. It was basically like a fake thing.*
>
> **Micro Business**

5.3.4 Brand impersonation

When considering brand impersonation, advertisers defined this as the unauthorised use of significant elements of their own brand by another party, including copying brand names, distinctive colours, logos and other recognisable assets without permission. Much like scams, the goal of brand impersonation was felt to be about misleading a consumer into buying fake products, low-quality products, and/or not receiving a product at all. Advertisers acknowledged that these types of ads could also damage consumer trust overall and there could be consequences for their own brand, for example losing sales to fraudulent actors and potentially suffering reputational damage.

There was general agreement that whilst brand impersonation may be difficult to proactively prevent, it was comparably easier to 'prove', particularly where cases involved copyright infringement.

MINI CASE STUDY

An advertiser from a large retail company discovered that a fraudulent company was mimicking their company's brand and running ads online directing people to a fake website which copied their name and logo. Customers expecting to make authentic purchases would then message the retail company on Facebook to complain about never receiving the items they had 'purchased' on the scam site. The advertiser said they had to repeatedly report several of the different scam ads when they saw them in order for the platform to take action as they did not know how else to resolve the issue. It took several weeks for the fraudulent site to be taken down.

> *Last year we found a fraudulent website that was promoting themselves as us… [customers] would then purchase from the scam website and then obviously they wouldn't get the product because you know, it's not a real website. And then they would come to our Facebook and complain that 'I ordered from you guys and I didn't receive anything'. So, it's impacting us on a wider scale.*
>
> **Large business**

5.3.5 Account takeover or 'hacking'

Various advertisers reported instances of account takeover, by which they referred to 'bad actors' logging into the business' ad accounts, locking legitimate users out, and in the worst cases, threatening the organisation with ransom demands in order to restore access.

Some platforms (for example Meta) were perceived to be more 'at risk' to attempts of account takeover than others. Multiple advertisers reported receiving an increased number of attempted 'phishing emails' pretending to be from Meta Ads Manager which had caused them to approach any communications from the platform with an increased level of scrutiny.

Whilst instances of account takeover could be challenging to resolve due to slow reporting processes, there was a general sense that account takeover was the most proactively managed type of fraudulent activity. Increased use of MFA, business accounts, as well as established internal data protection policies and training to mitigate against phishing attempts (especially in larger businesses and media agencies), felt sufficient preventative measures and advertisers struggled to see what more could be done in this area.

> *[A hacker] sent an email that looked like it was from Meta to my social media manager. She clicked it, unfortunately, and that's how they were able to access the account. The hacker had taken over the page and put a new page up…It was a nightmare because Meta was an absolute nightmare to deal with. It took 12 weeks to resolve, which I thought was totally unacceptable.*
>
> **Medium Business**

MINI CASE STUDY

A media agency's client clicked on a link in an email claiming to be from 'Meta Ads Manager support'. A hacker managed to gain access to the account. The hacker ran a scam campaign on the account, selling two pairs of 'shoes' for £9000. They said the issue took a while to be resolved and, in the end, the advertiser found the bank felt more helpful than Meta as the bank was able to block the company's bank account remotely.

Media Agency

5.4 Reporting fraudulent advertising

The process for reporting fraudulent advertising (including scams, brand impersonation, account takeover) was felt to present significant challenges. Processes across platforms were widely perceived as inconsistent, cumbersome, and unhelpful and advertisers felt there was a correlation between advertising spend and the ease of reporting fraudulent content. Reporting procedures were felt to present substantial opportunity for regulatory improvement, which is explored further in Section 6.

Businesses with higher advertising expenditure – typically larger businesses and media agencies – reported simpler and more efficient reporting processes. These businesses felt they directly benefited from closer, more direct relationships with the platforms via dedicated account managers who could be contacted directly by phone or email to report issues as and when they occur. This personal point of contact was felt to streamline the resolution process, with some reporting issues being resolved within a few days.

> *It can be really difficult for clients to access Meta support. I've had people refer to me a lot to sort out that sort of stuff and help them with it.*
>
> **Media agency**

In contrast, businesses with lower advertising spend – typically smaller and medium-sized businesses – reported experiencing confusing and often cumbersome reporting processes with significantly longer resolution timelines. These advertisers felt there was a lack of clarity in terms of how to report, who to contact, and how long the resolution will take. This was felt to be the case across platforms and ecosystems. This uncertainty created a sense of frustration and left those impacted by fraudulent advertising in limbo for extended periods whilst awaiting a response or outcome from the platform.

> *It took ages to resolve. Trying to prove that we were the rightful owners of the account. It wasn't good customer service process at all.*
>
> **Small Business**

6 The future role of regulation in relation to fraudulent advertising

6.1 Overview

This section examines advertisers' attitudes toward potential regulatory measures relating to fraudulent advertising, alongside the measures advertisers believed platforms, and Ofcom, could implement or improve on to address issues related to fraudulent advertising and other problematic activity online.

6.2 Overall attitude to further regulation in relation to fraudulent advertising

Advertisers acknowledged that protecting and mitigating against fraudulent activity online was important and an area that required consistent regulation, be that from Ofcom or trading standards bodies. However, despite many advertisers having experienced fraudulent advertising second-hand and/or been victims themselves, there was some hesitancy about introducing further regulation in this area.

Advertisers' hesitancy was driven by several key factors:

1. Firstly, addressing ad fraud and sharp practice felt more top of mind than scams, brand impersonation and account takeover due to the perceived salience of impact and ease of policing as explored in Section 5 of this report.

> *We worked with a partner. We spent six grand a year on them. They blocked bot traffic and said they were blocking a lot. Google says, 'no they're not bots, we charge you money for those, they're real'.*
>
> **Large business**

> *I have noticed some advertisers within our sector sort of copying our ads. So, they'll take our ad and put their own spin on it, but you can clearly see that they're copying our ads.*
>
> **Small business**

2. Secondly, there was a general sense amongst advertisers that online safety and security appear to be improving within the online advertising environment and beyond. Whilst the online world can feel challenging to monitor and regulate given the number of active users and pace of change, advertisers felt that the enhanced use of AI presents opportunities to monitor more closely 'at scale'. Advertisers felt there was also a wider societal shift to strengthen online practices and processes, and it is likely that it will continue moving in that direction as fraud and scams get more sophisticated. The prevalence of MFA use in their professional and personal lives was cited as an indicator of this shift.

> *I've noticed more recently that when you publish campaigns or logging into accounts, it'll quite often ask you to verify who you are before it lets you do things. That'll be a text or WhatsApp or an email.*
>
> **Media agency**

3. Finally, advertisers expressed some scepticism, and often nervousness, about the potential effectiveness of any new measures in this area. Beyond the existing infrastructure (namely MFA and platform ad reviews), most struggled to envisage what additional meaningful checks could be introduced that would not significantly disrupt their day-to-day workflow. Whilst advertisers could appreciate that prevention of fraudulent advertising was important for their business and consumers more widely, there was nervousness about what that might look like in practice as most wanted to avoid significant extra friction in the process.

> *If I had to do it [MFA] every time, it would probably become a little bit tiresome. So, there is kind of a limit in terms of happy to do it and happy to use a sort of a code generator every time, as long as it lasts for 24 hours or something like that so I can get through the workday. Because I might log into something 20 times just for, oh, I just need this one number or whatever it is. And to do it every single time is a bit tedious. Or if you don't have your phone.*
>
> **Medium business**

> *I'm just continuously chasing codes around … there's so much that is there on a security front and it needs to be. But it just gets very tiresome very quickly.*
>
> **Small Business**

6.3 Principles to consider

Taking all the above into account, there were two core principles that advertisers felt should be considered when introducing or making improvements to safety and security measures in the online advertising journey:

1. **Ensure any measures are not too onerous**. Advertisers accepted that a certain number of checks, especially when advertisers are onboarded to platforms (for example, ID verification, providing company documents), are necessary and important. Alongside this, risk-based, proportionate checks felt reasonable and vital to maintain (for example, scrutinising newer accounts, additional checks for regulated industries). However, there was resistance to introducing new checks that may add unnecessary friction to the process, for example, requiring advertisers to re-authenticate at multiple points in the process or multiple times during the day.

> *I've not come across that many issues really. I think I wouldn't want to see any more security measures because then you're sort of taking time away from the advertisers to go through all these different checks, all these different things.*
>
> **Small Business**

2. **Ensure humans remain at the core of any measures.** Advertisers acknowledged that enhanced use of AI provides an opportunity for safety and security to be more actively maintained at scale. However, there was a strong desire for humans to remain at the core of any measures, for example, making the judgement call on complex ad reviews or appeals of paused/flagged content, as well as in customer service engagements such as reporting account takeovers.

> *I think AI is doing the review. I can't say I'm confident in AI. I feel like it needs a human. A lot of the time, it gets taken down and then gets reversed when a human is looking.*
>
> **Large business**

6.4 Potential measures

When considering the future of safety and security measures to prevent formal fraudulent advertising, most advertisers felt that change should be focused on improving existing processes, rather than introducing entirely new measures.

6.4.1.1 The reporting process

The area that felt most in need of improvement was the reporting process, this included:

- Clearer signposting of where to go to report fraudulent advertising, ideally with dedicated channels for different issues (including a channel for reporting sharp practice, as well as 'official' fraudulent advertising).
- An option or ability to speak directly to a human, rather than engaging purely with chat bots or technology throughout.
- Faster resolution timelines, particularly in cases of account takeover which could have significant commercial implications for brands.

There was an overarching call for improved transparency and equity on how platforms triage and address reported issues. Whilst most appreciated that it was unrealistic for all advertisers to have an Account Manager, they felt it was important that regardless of ad spend, all legitimate advertisers should have the option to speak directly to a human and that all should be treated with the same urgency.

> *They could have a dedicated number or something that you can ring. You should be able to speak to someone straight away about it. You shouldn't have to go through all these steps. It was so difficult to find where you had to log it and the whole process was quite complicated. They should be much better.*
>
> **Medium business**

Beyond the reporting process, advertisers referenced three other potential areas of improvement at different points in the online advertising journey. These are explored in Sections 6.4.1.2, 6.4.1.3 and 6.4.1.4 below.

6.4.1.2 Account set up

Advertisers were open to more stringent checks at onboarding, with all platforms required to collect comprehensive information about the company (e.g. company registration numbers, VAT numbers, trademark information). Advertisers were also accepting of a delay (days to 1-2 weeks), between opening an account and being able to advertise for comprehensive checks to be conducted.

There was some appetite for 're-verification' on a periodic basis for all accounts (for example, once every one to two years), and scrutiny on dormant accounts. As part of this, it felt important that re-verification was not too frequent and that any documents provided were comprehensively reviewed (ideally by a human). Some felt companies should be cross-checked against their activity on other platforms to identify repeat 'bad actors' (i.e. ensuring accounts cannot be removed from one platform for malpractice, and easily set up on another).

> *I would be totally happy for additional checks to be in place, particularly in the setup side of things, absolutely […] if it was quarterly or every half year, I think I would get frustrated.*
>
> **Media Agency**

6.4.1.3 Day-to-day Management

Advertisers felt that MFA should be mandatory across platforms (if that is not already the case), and that it should be triggered when a user is logging into the account as well as when making more significant (and potentially riskier) changes to the account, for example changing the bank account details or budget.

Advertisers felt that verification should involve another individual in the company where possible when making more significant changes to the account, for example by sending a code by email to someone who has been selected as responsible for sign off.

> *I think it would be great actually if they demanded that everyone who was running ads had to do two-factor authentication.*
>
> **Media Agency**

> *I believe it has become mandatory. I think it started by recommending you switch it on so I switched it on for all the accounts, but if I'm not mistaken, of late, it's become mandatory. I'm not 100% sure on that.*
>
> **Large Business**

6.4.1.4 Posting an Ad

Advertisers felt it was important that platforms continue to spot-check and review ad content before ads go live. However, they felt this process could be improved by:

- Providing more clarity on why ads are rejected, including a more detailed, specific explanation for the rejection and indication of which part of the ad is causing the issue.
- Requiring advertisers to verify any significant claims made in ads (e.g. claims that a product will yield a certain result); this could also support with addressing the issue of sharp practice.
- Balancing the use of AI with human oversight and judgement calls more carefully to avoid AI rejecting ads due to minor points or misunderstandings.

Beyond this, advertisers felt platforms should be required to be more transparent and proactive in relation to 'ad fraud', including bot and click-fraud detection.

> *I was very surprised about not having to verify any of the claims you're making, especially if you're selling a regulated product.*
>
> **Medium business**

7 Appendix

7.1 Sample breakdown

7.1.1 Sample for the digital task

Audiences	
Larger businesses	7
Medium businesses	9
Small/micro businesses	13
Sole traders	4
Businesses who outsource to an external company	3
Media/ad agencies who run ad campaigns on behalf of other businesses	4
Region	
England	24
Wales	5
Scotland	4
Northern Ireland	3
Ad Spend	
Low (£0-£25k p/a)	12
Med (£26-£100k p/a)	6
High (£100k+)	18
Sector	
Leisure/Entertainment/Hospitality/Lodging/Restaurant	4
Medical/Dental/Health services	3
Computing/I.T.	4
Real estate and utilities	1
Education	1
Non-profit	1
Gambling	1
Professional or business services (e.g. employment agency)	4
Retail/Wholesale/Distribution	9
Green Sector + Freelancer	1
Manufacturing	1

Finance/insurance (not at a bank)	2
Banking/credit cards	1
Automotive services and/or auto sales	1
Health and wellness/Tech	1
Telecommunications or utilities	1
Transportation/Logistics/Travel Agency	1
Personal care and beauty services	2

Platform	Used in last two months	Use in next two months
Facebook	31	31
YouTube	18	17
Instagram	29	27
Snapchat	2	2
LinkedIn	15	16
X	2	2
TikTok	16	18
Google Search	24	25
Pinterest	2	2
Reddit	8	6
Types of ads	**Used in last two months**	**Use in next two months**
Search	24	30
Display	27	25
Classified	2	5
Boosted	29	27
Ad ecosystems	**Used in last two months**	**Use in next two months**
Walled garden	36	34
Open web	28	30
Hybrid	5	3

7.1.2 Sample for the follow-up in-depth interviews

Audiences	
Larger businesses	7
Medium businesses	5
Small/micro businesses Sole traders	9
Businesses who outsource to an external company	0
Media/ad agencies who run ad campaigns on behalf of other businesses	4
Region	
England	15
Wales	3
Scotland	2
Northern Ireland	1
Ad Spend	
Low (£0-£25k p/a)	4
Med (£26-£100k p/a)	3
High (£100k+)	14
Sector	
Leisure/Entertainment/Hospitality/Lodging/Restaurant	3
Medical/Dental/Health services	3
Computing/I.T.	1
Non-profit	1
Gambling	1
Professional or business services (e.g. employment agency)	2
Retail/Wholesale/Distribution	3
Green Sector + Freelancer	1
Manufacturing	1
Finance/insurance (not at a bank)	1
Banking/credit cards	1
Automotive services and/or auto sales	1
Telecommunications or utilities	1
Personal care and beauty services	1

Platform	Used in last two months	Use in next two months
Facebook	20	19
YouTube	12	11
Instagram	18	16
Snapchat	1	2
LinkedIn	7	8
X	2	1
TikTok	12	13
Google Search	17	16
Pinterest	1	1
Reddit	7	5
Types of ads	**Used in last two months**	**Use in next two months**
Search	16	18
Display	17	15
Classified	1	3
Boosted	19	16
Ad ecosystems	**Used in last two months**	**Use in next two months**
Walled garden	21	20
Open web	19	19
Hybrid	2	1

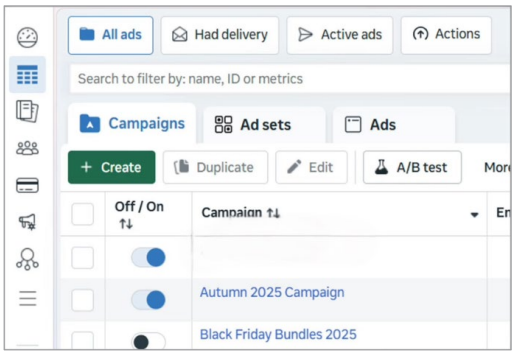
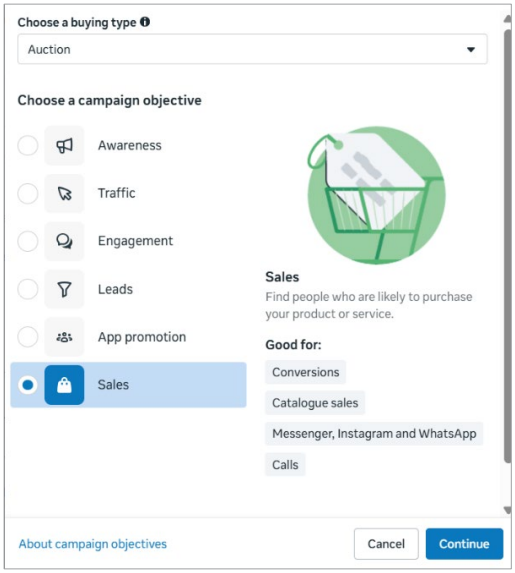
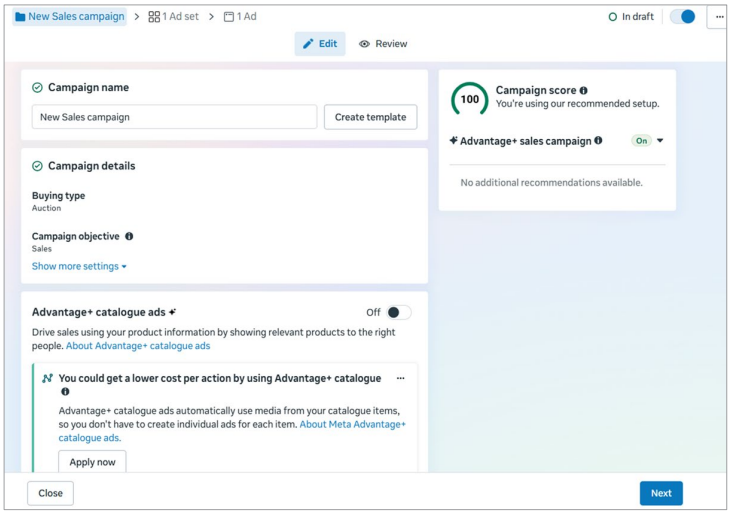
7.2 Ad journeys

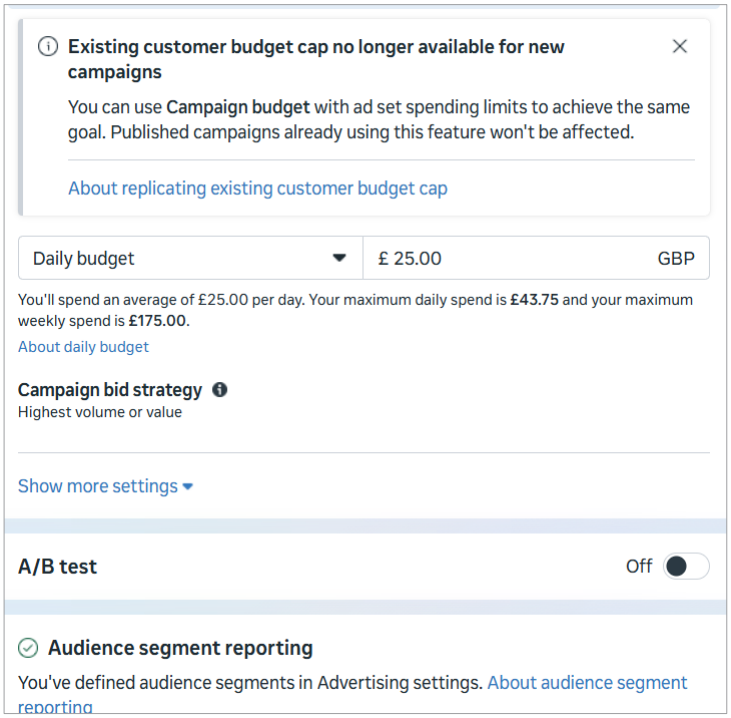
The below sections include screenshots and quotes submitted by advertisers as part of the digital task to illustrate the online ad pathway across different platforms. Some images are blurred for data protection reasons.

7.2.1 Meta Ad Manager

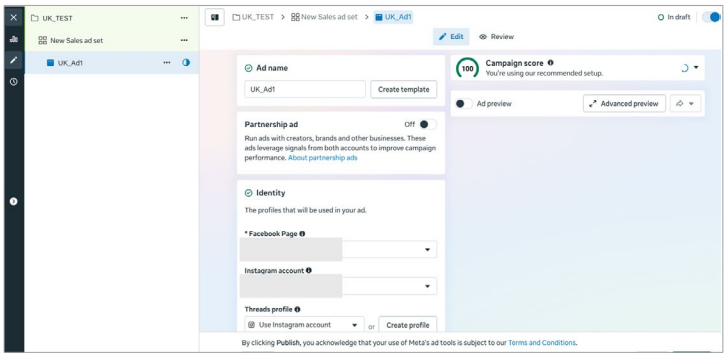
Below is an example from an advertiser working in a Medium sized business launching an ad campaign on Meta Ads Manager using a Business Account.

Step Title	Screenshot from advertiser	In the words of the advertiser
Step 1: Log into account – 2FA required	N/A	"When I log in, I have to do a 2-FA to make sure it's me. I login with my password and

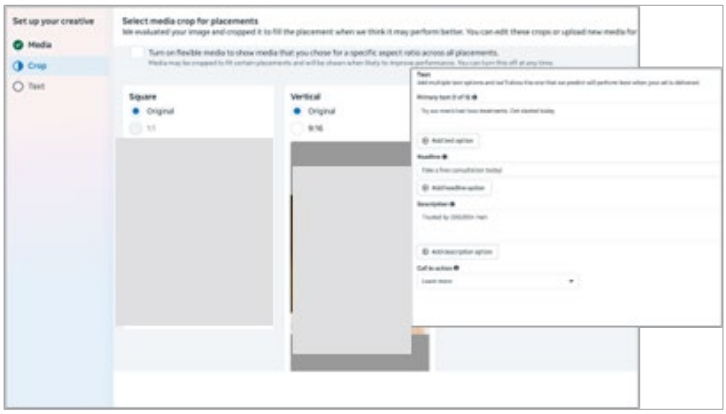
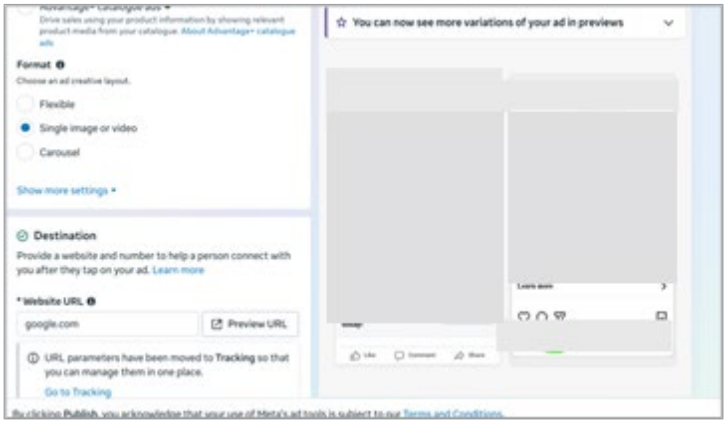
		then I get a passcode to my app on my phone.”
Step 2: Create Campaign and Set Goal	 	“Once I am in the platform, I click the “Create” button to create a new campaign. I am then prompted which campaign goal I am after. In this case (and in most cases) I select sales.”
Step 3: Adjust settings and set budget		“Next, I set things like the budget, campaign objective and if I want to use 'advantage catalogue plus ads' which is a feature that utilizes our product feed. I also have the option to select if we fall under the 'special categories' but we do not as this is primarily political ads or finance related ones.”



Step 4: Set ad group: choose name, target audience, profiles, location



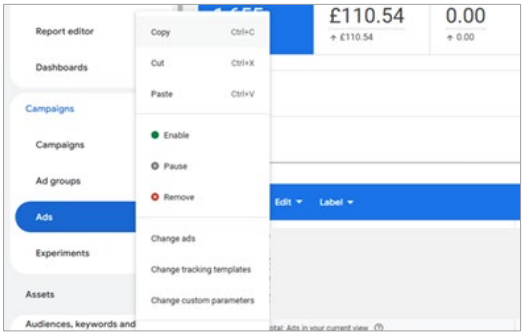
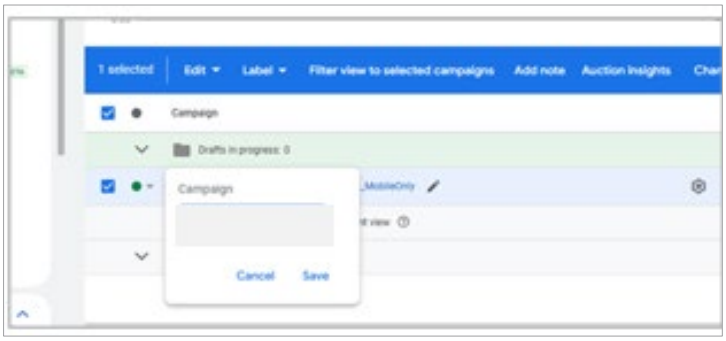
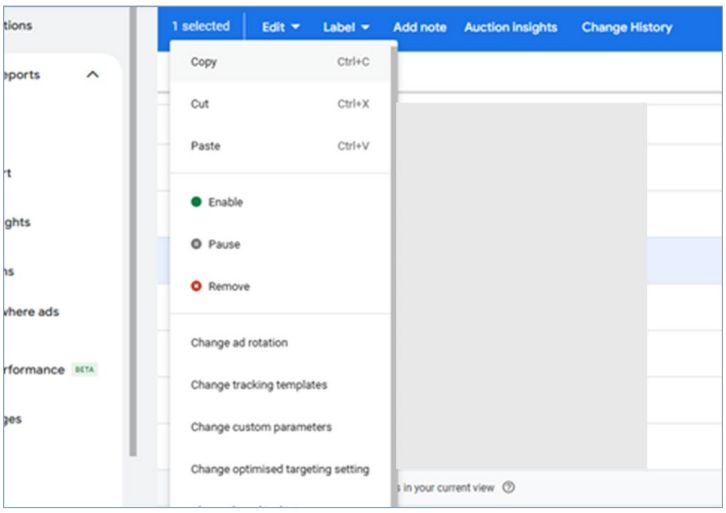
"I then move to ad group settings. This is more for the audience we are targeting. Generally, I keep our targeting broad. The main one I change is gender which I set to men as we only sell [male products] so targeting women is no use and a waste of spend. I can also select the attribution model I want. I normally go for click only attribution as view only feels like a waste of money. I also set the location to the UK as this is where I want my ads to show."

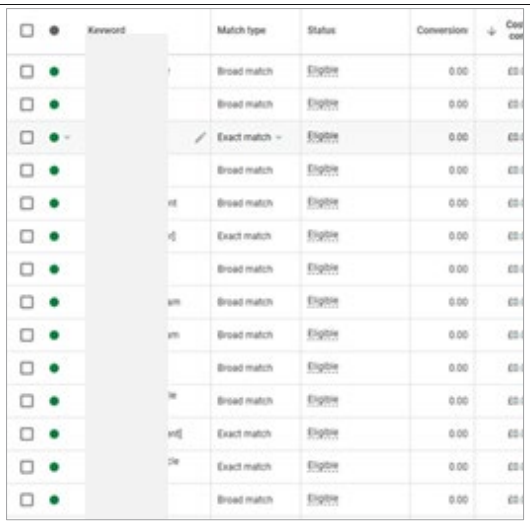
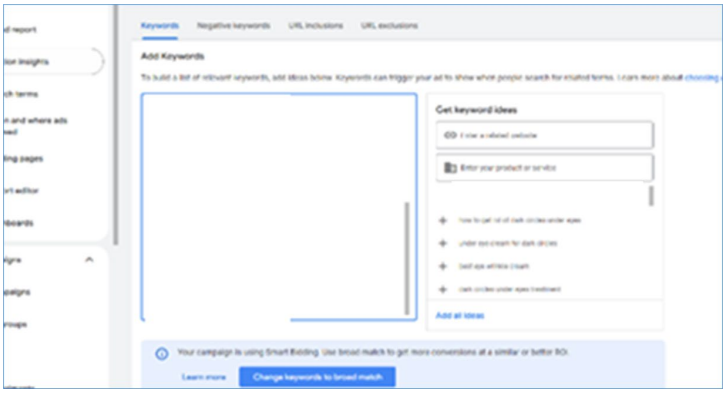
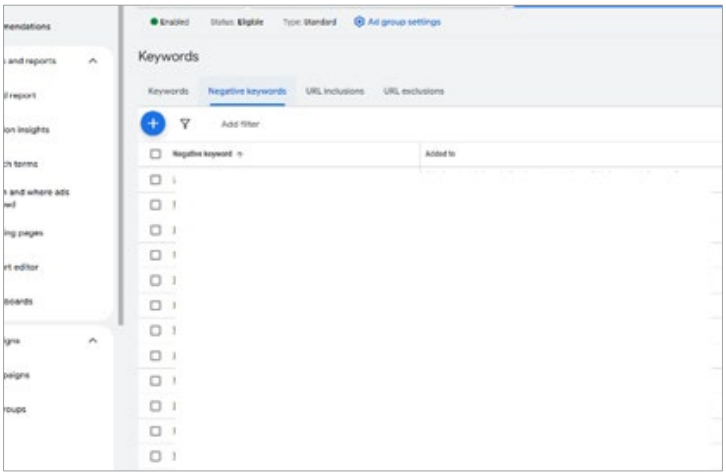
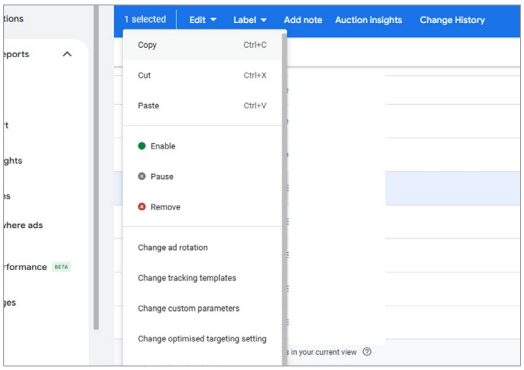
Step 5: Upload chosen media and supporting text		“Once this is done, I can move to the ad creation part. All parts before this are quite quick, but this often takes the longest. I start by naming the ad and then going to 'add media' and can upload a video. Once I have uploaded the file, I select it and go to the next stage. Here I have the option to crop my video to make sure it fits all the different formats. Once this is done, I go to the next stage which lets me write the body copy. This is pre-done and is usually copy and pasted in from a word doc.”
Step 6: Add URL and publish – add is ‘reviewed by Meta’ before going live		“Once this is done, the ad is created. The only final touches to make are adding in the URL we are going to send people to. For sake of this task and for privacy, I have put Google in the screenshot. Once this is done, I can hit publish and the ad will be reviewed by Meta before going live.

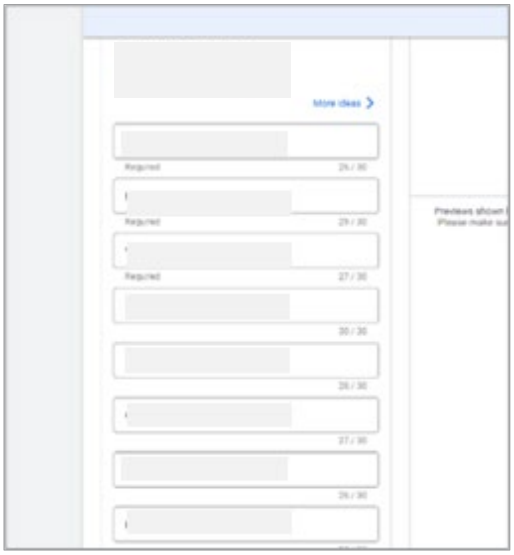
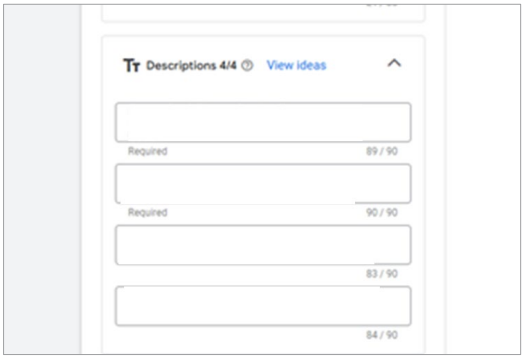
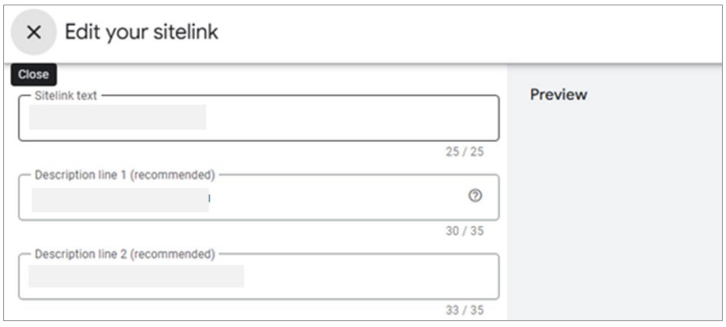
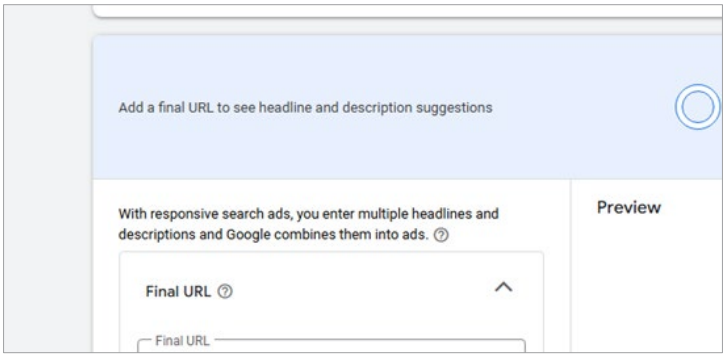
		There are no additional checks. Sometimes I get a warning about the format of the ad once it's been reviewed – e.g. it is not suitable for Instagram reels and then they prompt me to add another version."

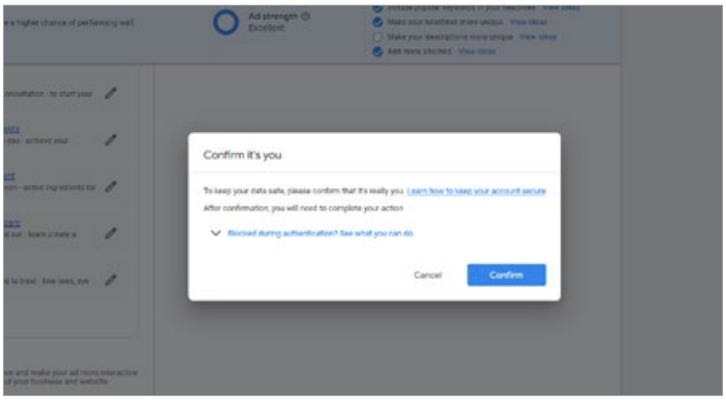
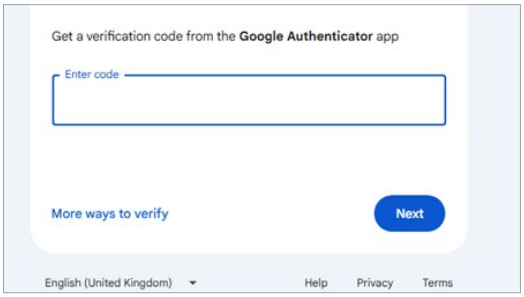
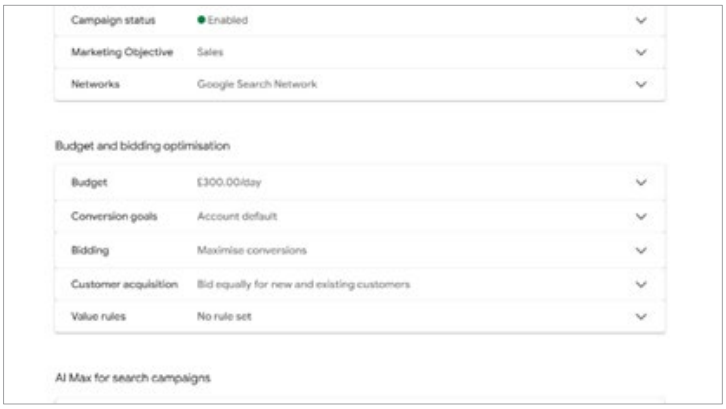
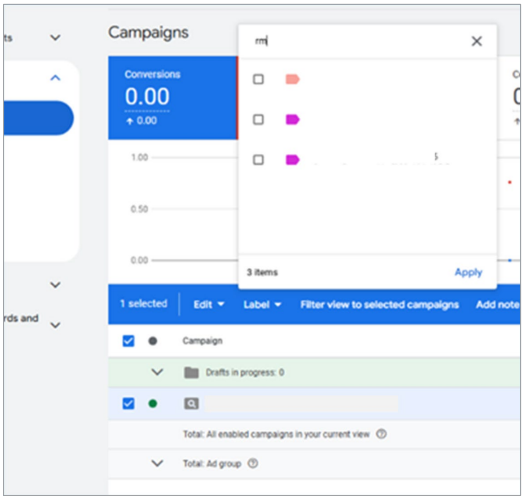
7.2.2 Google Ad Manager

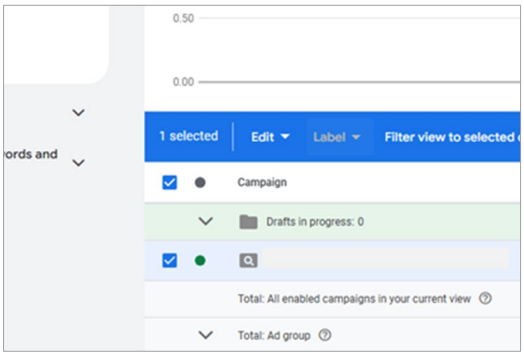
Below is an example from an advertiser working in a Medium sized business duplicating an ad campaign on Google Ads Manager using a Business Account.

Step Title	Screenshot from advertiser	In the words of the advertiser
Step 1: Duplicate Existing Campaign		"Step one is duplicating the existing campaign. I copy and paste existing campaign to keep existing campaign settings and ad settings. Takes 2 mins. Easy to do."
Step 2: Update Campaign name		"Then change the name of the duplicated campaign. I click the pencil to change the name to the new campaign and click save. Takes 1 min. Easy to do."
Step 3: Duplicate and rename the ad groups		"Then I select the desired ad group to copy. Click edit and then copy. Once copied, I will edit and paste again to create another ad group. Takes 5 mins. It's easy to do. Then I click on the pencil next to the name to change the name based on the theme of the ad group. Repeat this for desired number of ad groups. In fact, 5 duplications. Takes 5 mins. Easy to do."

		
Step 4: Add keywords		"After keyword research, I navigated to keywords by clicking on the ad group and pressed the plus button, then added the relevant key words for each ad group – bot exact and phrase match, using a keyword wrapper tool found online. Takes 5 mins. Easy to do."
Step 5: Add 'negative keywords'		"I then added all keywords for the other 4 ad groups as exact match negative keywords at an ad group level to avoid both ad groups showing up for those searches. Took 15 mins. It's straightforward but repetitive, copying and pasting back and forth."
Step 6: Duplicate old ads		"Then, I navigate to the ads. Select the existing ad and press copy. Once copied, paste the ad. 2 mins. Easy to do."

Step 7: Update Headlines		"I click the edit pencil to edit the ad and add relevant headlines to the ad to communicate features and benefits and improve the ad score by matching to keywords in the ad group. Takes 15 mins. Simple process – takes time to think about the best headlines."
Step 8: Update Descriptions		"Then I update the descriptions. Takes 10 minutes. It's simple but takes time to think about the best descriptions."
Step 9: Update Sitelinks		"I'll then update the sitelinks. I edit sitelinks that aren't relevant to the ad groups so that there are no links that would take a customer to an irrelevant part of the website. 10 minutes of time. Simple process but takes time to think about relevant sitelinks. I'll then paste URL into URL box. 1 min. Easy to do."
Step 10: Update URL		"I paste URL into URL box.1 min. Easy to do."

Step 11: Save ad	 	"At this point I was prompted to confirm it was me by entering an authenticator code from an authenticator app. 2 mins. Easy to do."
Step 12: Check campaign settings		"Then it's check campaign settings. Including budget, marketing goals, bid strategies.3 mins. Easy to do."
Step 13: Label new campaign for tracking		"Then I check the settings including budgeting, marketing goals, big strategies. 3 mins. Easy to do."

Step 14: Final Checks		"I double check everything is correct before spending. About 5 mins. Easy to do."
Step 15: Set the campaign to 'Live'		"I change the status from 'paused' to 'active'. 10 seconds. Easy to do."

7.2.3 LinkedIn

Below is an example from an advertiser working in a Large business launching an ad campaign on LinkedIn using a Business Account.

Step title	In the words of the advertiser
Step 1: Define campaign objective and gather ad content	"I first clarify what the ad is for and what I want it to achieve. For example: generate leads, promote an event, increase brand awareness, or drive traffic to a specific landing page. Then I collect all the relevant information that needs to go into the ad(s), such as: Campaign objective and key message; Main value proposition/benefits; Any offers (discounts, free trials, downloadable content, etc.); Landing page URL(s); Approved logo and brand assets; Images/graphics or video for the creative; Ad copy ideas (headline, intro text, call-to-action); Any mandatory wording/disclaimers I usually consolidate all of this into one place (e.g. a document or folder) so that when I log in to the platform, I already know exactly what I'm going to say and show in the ad. Usually takes a few hours end-to-end, depending on how much information I already have and if I need approvals or input from others. It is easy, if all the information and assets are available and approved. It becomes more time-consuming if I'm chasing images, copy approvals, or links. Spending enough time here makes the later steps much smoother. If the content is not clear, it's harder to make good targeting and budget decisions later."

Step 2: Upload the campaign information to the platform	"I log in to LinkedIn Campaign Manager and select the correct account (e.g. the right company or ad account); click on "Create" → "Campaign" (or similar, depending on the UI); enter the campaign name so it's easy to recognise later; choose the campaign objective that best matches what I want (e.g. Website visits, Leads, awareness etc.); start filling in the basic campaign details, such as language, LinkedIn Page, and any initial settings required before moving to targeting and budget; begin uploading or attaching the ad content I prepared (e.g. headlines, primary text, URL, images/video, call-to-action). Usually takes roughly 20–30 minutes, assuming I already have all the content ready. It's easy to moderate. It's straightforward if you're familiar with LinkedIn's interface, but it can take a bit of time to double-check that all fields are correctly filled, especially if there are multiple ad variations. A clear naming convention and organised files make this step much faster. Also, I try to keep copy fairly short and to the point, because LinkedIn truncates longer text."
Step 3: Define and allocate target audience	"After the basic information is uploaded, I configure who I want to see the ads. On LinkedIn this involves: Select locations; choose relevant demographics such as job titles, job functions, seniority, company size; add industries or sectors that match the campaign; include interests, skills, and groups that align with the ad (e.g. "Digital Transformation", "Automation", "HR Technology"). I use 'exclude' options if needed (for example: exclude students, irrelevant industries, or job titles). Then I check the estimated audience size to make sure it's not too broad or too narrow, then tweak settings until it looks right. Typically takes 15–30 minutes, depending on how refined the targeting needs to be and whether I test different combinations. It feels moderately easy. The options themselves are clear, but it takes some thought to balance being specific enough to be relevant without making the audience too small. Getting targeting right is crucial. I often cross-check the audience size and selection with my campaign goals and, if possible, with colleagues who know the market well."
Step 4: Set campaign budget, schedule, and bidding	"Once the audience is defined, I configure how much we are willing to spend and over what period: Set the campaign budget based on what has been approved internally (e.g. daily budget or total budget for the whole campaign). Choose whether the budget is daily, lifetime, or a mix (depending on how LinkedIn presents the options). Set the start date (and end date if the campaign is time-bound, like an event). Review or adjust the bidding strategy (for example: manual bid vs automated/maximum delivery, depending on what's available and recommended). Make sure the estimated spend and duration match what has been agreed with stakeholders or management. Normally takes 10–15 minutes, since the amount is usually decided beforehand and I just need to input it correctly.

	Easy, provided the budget has already been approved. The only complexity is understanding the difference between daily vs lifetime budgets and how LinkedIn distributes the spend. I double-check the currency and total amount carefully, because a small typo here can significantly over – or under-spend the campaign.”
Step 5: Final review and launch the campaign on LinkedIn	“What you had to do: Before launching, I go through a final checklist: Preview the ads to make sure images, text, and links look correct on both desktop and mobile. Test that the URL works and loads. Review the audience settings one more time (locations, job titles, industries, etc.). Confirm the budget, dates, and bidding. Check the campaign objective is aligned with the actual goal (e.g. lead gen vs traffic). Once everything is confirmed, I click “Launch”/“Publish”. After launching, I keep an eye on performance in the first few days to ensure impressions look reasonable. The final review and launch usually takes around 5–10 minutes. Easy, as it’s mainly checking and confirming details already entered. The main risk here is human error (wrong link, typos, incorrect targeting), so taking a few extra minutes to review everything carefully is worth it before pressing ‘Launch.’”
Comments on safety/ security checks throughout the process:	“I didn’t encounter any unusual safety or security checks beyond normal LinkedIn login and occasional re-authentication, which felt straightforward and reassuring. Billing was already set up on the account, so there were no extra payment verifications. During setup, LinkedIn showed helpful prompts about audience size and budget (e.g. if targeting was too narrow or the budget might limit results), but these were advisory, not blockers. After launch, the ads went through the standard LinkedIn review process for policy compliance; my ads were approved without any warnings or rejections. Overall, the safety and policy checks felt smooth, light-touch, and supportive rather than restrictive.”

7.2.4 TikTok

Below is an example from sole trader launching an ad campaign on TikTok using a Business Account.

Step Title	In the words of the advertiser
Step 1: Log into account – CAPTCHA	"There is option to set up 2-factor authentication, but I don't have it set up at the moment. Right now, it will ask for username, password and then it's a robot check. You have to identify this image as the same as another. You always have to do that on TikTok.
Step 2: Create campaign	I scroll down and select 'SHOP ADS.' Then I click on CREATE GMV MAX ADS"[3]
Step 3: Adjust Campaign Settings and set budget	"I select PROMOTE PRODUCTS, select which products I want to promote and then enter a budget per day, ROI and number of days"
Step 4: Finalise campaign and publish	"Finally, I choose which Ad creatives to use, these can either be uploaded or auto selected. After choosing my creatives, I click publish."

7.2.5 YouTube

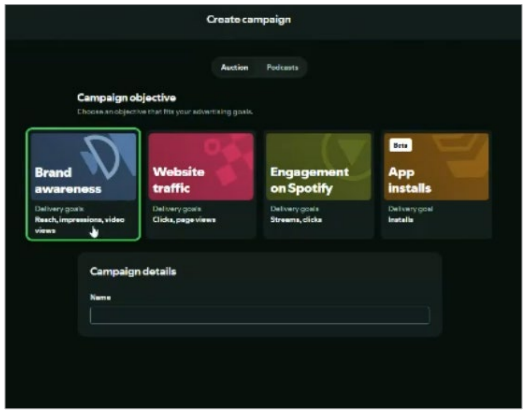
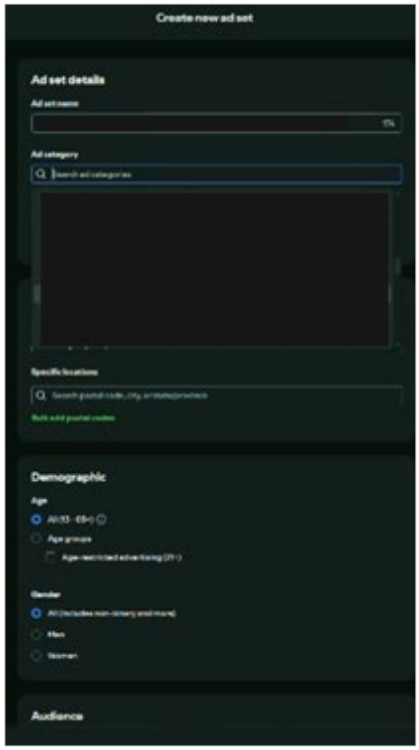
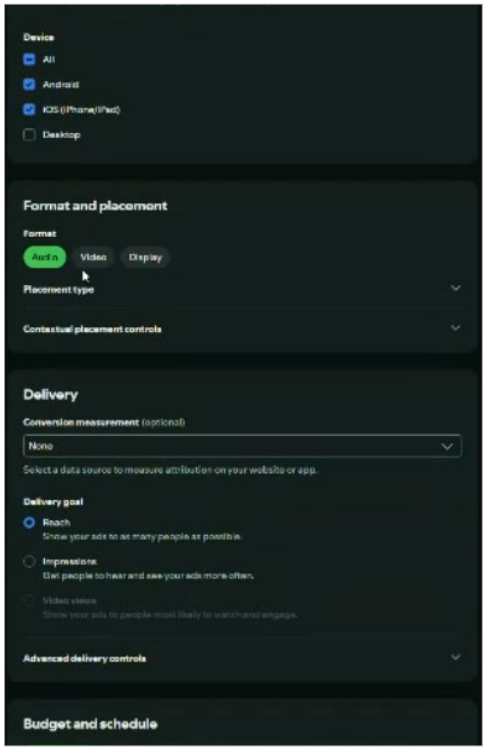
Below is an example from media agency 'boosting' content as a paid-for campaign on YouTube on behalf of a client.

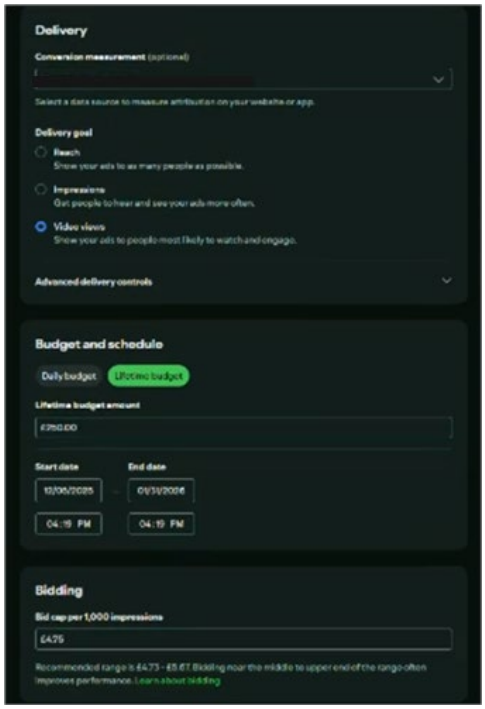
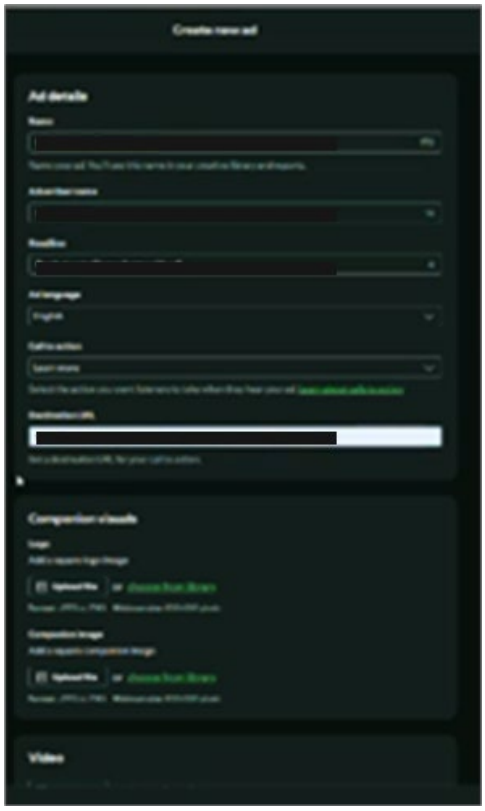
Step Title	In the words of the advertiser
Step 1: Log into account – 2FA required	"Sign into the platform – i.e. YouTube Studio. We've got a lot of 2FA set up which is good. I think it's more of a recommendation than a requirement."
Step 2: Create campaign	"Then I find the video tab and content tabs. I select the relevant video and click 'promote' in the hamburger."
Step 3: Adjust Campaign Settings	"Then I set the goal (i.e. more views), define who I want to target and set the length of time/how long I want the campaign to run for."
Step 4: Finalise budget	"Then I'll select the payment account and authorize payment."
Step 5: Launch campaign	"I then finalise and launch the campaign"
Comments on other safety/security checks on YouTube:	"On YouTube, you've also got the copyright issues to deal with. Sometimes you have to persuade them that it really is you singing your own song. There may be a claim against something and you have to provide various tick boxes to say 'this is us'. You submit links and then somewhere in the magic back of it all, it tends to resolve itself."

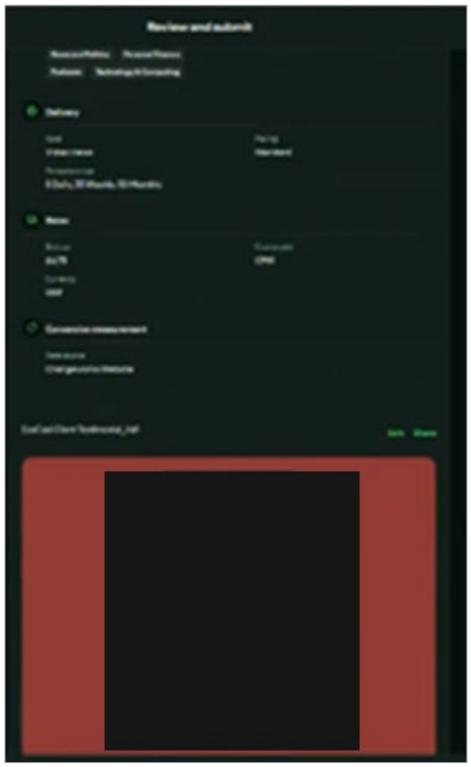
[3] GMV Max ads was described as a TikTok feature that automates ad creation and optimisation for TikTok Shop sellers.

7.2.6 Spotify

Below is an example from an advertiser working at a medium sized business launching an ad campaign on Spotify using a Business Account.

Step Title	Screenshot illustration and/or words of the advertiser
Step 1: Log into account – 2FA required	"All of our accounts have multi-factor authentication. They will text me with a code."
Step 2: Choose campaign focus	
Step 3: Adjust Campaign Settings	 

Step 4: Set budget and schedule/timings	
Step 5: Add headline, description and URL	

Step 6: Review and submit campaign	
Overall comments on other safety/security checks:	"I'm going to be brutally honest, they [ad platforms, in general] are completely pants. If I can get an email that remotely relates to the organisation you're trying to impersonate, I could get a verification code. The only one that is semi-decent is Google…but from other platforms, I could impersonate you within 24 hours and I don't think they would pick it up for weeks. "

Classification: CONFIDENTIAL

MRS Awards 2024 Winner Business Impact of the Year - UK
MRS Awards 2022 Finalist Business-to-Business Research
MRS Awards 2020 Winner Innovation of the Year
MRS Awards 2019 Winner Global Agency of the Year
MRS Inclusion Pledge

STRAT7 JIGSAW

Ofcom

Thank you

STRAT7 Jigsaw
A trading division of STRAT7 Limited

98 Theobalds Road, London, WC1X 8WB, UK

+44 (0)20 7291 0810

Web: www.jigsaw-research.co.uk
Email: info@jigsaw-research.co.uk

Registered in England no.: 7642707
Registered Address: 11 Soho Street, London W1D 3AD

VAT no.: 326 011 940

MAKING SENSE OF HUMAN COMPLEXITY