GENERAL GUIDANCE NOTE

Digital marketing and promotions

Digital marketing

In this context, digital marketing and promotions refers to a broad range of marketing practices that make use of online platforms. Many of these practices generate revenue for the industry and allow consumers to engage with premium rate services (PRS) as a payment method. Two commonly used methods are Affiliate Marketing and Direct Buy Marketing. This document focuses largely on Affiliate Marketing.

The PSA has produced an Annex to this document to support providers using Direct Buy Marketing.

Affiliate Marketing

Affiliate Marketing is where providers of phone-paid services contract their digital marketing to partners, the majority of which are known as 'affiliate marketers'. This is a legitimate practice which can provide value to providers of phone-paid services by leveraging external marketing tools and techniques paid for on a results basis.

However, for providers of phone-paid services it can also be a risky practice as there are often multiple parties in the value chain and it may be difficult for the provider to have control over the marketing practices that these parties employ. For example, the Level 2 provider may contract with an affiliate, who may then further contract with multiple other parties.

There are a range of different practices, some which are legitimate and able to satisfy the outcomes of the Code, and others which are high risk and less likely to be compliant. Further information on these is outlined below.

Some examples of practices which are legitimate and able to satisfy the outcomes of the Code are:

- Banner ads
- Pop-ups and pop-unders
- Search engine marketing (SEM) and search engine optimisation (SEO)
- Adware

Although the above practices can be undertaken in a way that is legitimate, there is still potential for consumer harm, and the Phone-paid Services Authority (PSA) has seen instances where consumers have been misled by marketing using these techniques in the past.

Examples of practices which are always capable of misleading if not treated with caution and control:

Typosquatting

Registering internet domain names that are misspellings of well-known brands. Consumers are taken to a promotional website following their typing error of a well-known online service – often consumers are not immediately made aware of their mistake and may associate such promotions with the service they were actively looking to reach.

Clickjacking

Consumers are induced into clicking on something that is different to what they perceive they are clicking on. By clicking on a disguised link on a web display the consumer triggers other internet functions. The consumer is unaware of what they are instigating and where such clickjacking is relied upon for consent, this is invalidated by the consumer's user experience and knowledge.

Likejacking

Similar to clickjacking, however the consumer is using commonly used social media functions as displayed on the screen – often the consumer is unaware at the time of the wider impact of their use of a social media application or their decision to 'like' a particular piece of social media content.

Content locking

Specifically this relates to marketing techniques used by one party, such as an affiliate marketer, to generate leads and increase conversions for a second party's online service transaction. Consumers are often induced to make the payment on the second party's website because they believe it is the only means of accessing the original party's content, and not because of any interest in the product or service for which they make payment. Furthermore, commission from the payment goes to the marketing affiliate to pay for content that may be presented as being "free".

This is not an exhaustive list. The market is constantly evolving and while the PSA will endeavour to keep the list as up-to-date as possible, providers should constantly be aware as to whom their services are marketed to online and whether these and other emerging practices are likely to meet the outcomes set out in the Code. Detailed examples of practices, including those mentioned above, that may cause a breach of the Code can be found in the Annex to this Guidance.

This Guidance also clarifies that it is the responsibility of providers to control affiliate marketing carried out on their behalf and sets out some recommendations as to how to do so safely. For further assistance on controlling risk when using affiliate marketers please read part 10 of the Promoting premium rate services Guidance.

When managing any digital marketing campaign, service providers should address potential risks by actively seeking to meet outcomes in the PSA's Code of Practice (the Code). In particular, service providers should give due regard to:

Transparency: consumers must be presented with all vital information, including the price, relating to a PRS service before they commit to purchasing it.

Fairness: if consumers are to have confidence in the PRS industry, it is important that they are not intentionally misled.

Privacy: consumers should be protected from an invasion of their privacy. Any promotional material must be delivered appropriately and with the consumer's consent, which must be knowingly given and clearly identifiable.

Businesses, advertisers and relevant trade bodies, such as the Internet Advertising Bureau (www.iabuk.net), are collectively seeking ways to improve the quality of digital advertising through a range of campaigns. These campaigns are frequently seeking to achieve similar outcomes as those set out in the Code so as to improve consumer experience and reduce the need for people to resort to ad blockers. We recommend service providers consider advice and support offered through such third parties.

How to manage relationships with affiliate marketers, lead generators and other digital marketing partners

Service providers often subcontract their digital marketing to partners, the majority of which are known as 'affiliate marketers'. This is an entirely reasonable and legitimate thing to do, and can provide value to providers by leveraging external marketing tools and techniques paid for on a results basis.

However, providers who use affiliate marketers need to be aware of two key points:

- Responsibility for ensuring that promotions are compliant with our Code remains with the service provider regardless of whether this activity is sub-contracted to a third-party such as an affiliate marketer. So if an affiliate marketer's activities lead to a breach of the Code in relation to a PRS service, then a Tribunal will generally hold the service provider accountable for the breach under the Code.
- Indeed, we have seen a number of cases where affiliate marketers have been responsible for misleading digital marketing practices of the kind outlined within the Annex to this guidance in an attempt to inflate their revenues by engaging consumers in services without their clear understanding and informed consent.

Providers therefore must put in place appropriate controls to ensure their affiliate marketing adheres to the Code as part of their ongoing compliance processes. The absence of any such mechanisms may be viewed by a PSA Tribunal as a failure of the provider to assess the potential risks posed by a party with which they contract and maintain steps to control these risks.

The PSA expects service providers to take account of the PSA's Due Diligence and Risk Assessment and Control (DDRAC) Guidance on clients. In particular, service providers should undertake effective due diligence on any affiliate marketer that they are seeking to engage.

As stated in paragraph 2.1 of the DDRAC Guidance, providers should seek sufficient information to assess the suitability of a new client. In the case of affiliate marketers, Level 2 providers might want to consider the following addition to ongoing considerations already set out in the DDRAC Guidance (the following is not an exhaustive check list but intended as a guide; we also recommend that providers keep an audit trail of any actions taken in order to minimise consumer harm in what is a high risk area):

- Companies checks
- Reputational checks through app stores, blogs, AV vendors, Level 1 providers etc.
- How established the affiliate network is
- Whether, according to any information that has been made available to the Level 2 provider or to industry more generally, the affiliate has been associated with any breach of the Code or any other related Codes of Practice or law – this, in particular, should be monitored on an ongoing basis
- Whether the affiliate marketer is aware of and committed to compliance with the legislative and regulatory landscape, i.e. the Code and other relevant codes and legislation including the Data Protection Act, Privacy and Electronic Communications Regulations 2003 (PECR), the Committee of Advertising Practice (CAP) Code and relevant consumer protection laws
- How the affiliate marketer sources its traffic; for example, does it source its traffic from file-sharing websites? Traffic should not be obtained from illegal sources.
- If the affiliate marketer sub-contracts with other affiliate marketers (which will amplify any risk), they too should be bound by contract to not obtain traffic from illegal sources
- Whether the affiliate marketer is willing to explain where and in what terms it plans to place your advertising and/or provide visibility of this retrospectively
- Using traffic monitoring using tools such as Alexa or SimilarWeb to understand how an affiliate generates traffic
- The level and sophistication of the tracking technologies the affiliate uses
- Whether the marketer in question has fraud detection systems and monitoring tools is place
- Whether the affiliate marketer is prepared to run its service on a trial basis where funds are capped until the relationship is fully established.

In addition, the PSA expects service providers throughout the value-chain to:

- Set clear expectations for their affiliate marketers around Code compliance and obtain a clear commitment to this end as part of any contract signed
- Ensure that affiliates will not engage in any of the misleading practices listed above or any other such misleading practices
- Closely monitor their affiliate marketing, particularly in response to consumer complaints, abnormal traffic patterns and where an affiliate marketer has previously been associated with a breach of the Code. We believe that effective monitoring and, as far as is possible, tracking are in the interest of the PRS industry.
- To this end, we recommend that providers analyse their traffic on an ongoing basis, responding to any abnormal activity and gaining an understanding of how consumers arrive at a promotion, and monitor and audit their affiliate marketing periodically regardless of activity to ensure that it is both effective and compliant. The Internet Advertising Bureau

(IAB) has produced a useful best practice guideline that may be a helpful starting point on how to conduct an affiliate audit albeit without informing your affiliates that you intend to conduct it.
- Make it clear to affiliate marketers that any failure to comply with the expectations set will result in suspension or forfeiture of payments, and reflect this in the contract.
- If an affiliate marketer is unable to meet the expectations placed on it, providers are advised to review their relationship with the affiliate marketer concerned. Keep clear records of any activity and make them available to the PSA upon request.

While we recognise that Level 2 providers generally contract with digital marketing partners, Level 1 providers are responsible for the risk assessment and control of their clients (i.e. Level 2 providers) to ensure that consumer outcomes outlined in the Code are met, including around their promotional material.

This is particularly important where a client is known to be using affiliate marketing. In such cases, the Level 1 provider should check that the Level 2 provider has appropriate controls in place and raise any issue of concern should one arise. We recommend that Level 1 providers conduct a range of auditable checks on their clients, including (but not limited to):

- Checking that the client has a satisfactory means of identifying inappropriate activity or significant risk by a specific affiliate. This does not necessarily have to name the affiliate, just allow the client to distinguish them from other affiliates who also provide traffic to them
- Ensuring the client has appropriate contractual arrangements and risk control processes in place to deal with affiliate marketing and misleading digital marketing more generally
- Undertaking thorough and frequent checks to ensure the client's promotional material meets the outcomes set out in the Code
- Monitoring activity for abnormal service behaviour on an ongoing basis and taking action upon it
- Generally ensuring that the client carries out the sort of due diligence, risk assessment, and control (DDRAC) processes set out in paragraph 2.4 above and paragraph 3.12 of the General Guidance note on DDRAC.

Examples of practices that may cause a code breach

These examples are provided to equip service providers across the value chain to manage the risks posed by digital marketing campaigns and develop promotional material that complies with the Code of Practice. By avoiding these practices, and taking steps to reduce the impact when third-parties use such practices without proper authorisation, service providers will improve compliance standards across the PRS market.

Typosquatting

Typosquatting involves registering internet domain names that are misspellings of widely known and trusted internet brands. Examples might include "Dacebook" instead of "Facebook", "Twtter" instead of "Twitter" and "Wikapedia" instead of "Wikipedia". This takes advantage of consumers who mistype or click on mistyped links by redirecting them from their intended destination. Consumers are then

led to a website that may be designed in a similar manner to the website that they were originally searching for.

In a PRS context, a consumer might be intending to visit a well-known website. However, having mistyped his or her intended destination into their browser's address bar, the consumer arrives at a website that may look like his or her intended destination but contains a PRS promotion. The consumer may pursue the promotion based on its apparent association with a trusted brand.

As set out in Rule 2.3.2 of the Code, providers should not mislead consumers. If a provider were to align itself with or imitate another brand with which it does not have an association, in a way that is likely to mislead consumers about the nature of the service being offered.

Corrective action will be necessary if typosquatting takes place to give the consumer a clear understanding of what has happened. While this may have an impact on conversions, such corrective action is required to meet the outcomes of the Code; or typosquatting avoided entirely.

Clickjacking

Clickjacking is a technique used to trick a consumer into clicking on something different from what they perceive they are clicking on. This is also known as 'user interface redress attack' or 'UI redress attack'. By clicking on a link that is obscured, masked or disguised consumers are redirected to a webpage that they had no intention of visiting. Users will often be unaware of the exploit as the link to the webpage they arrive at may be disguised as something else. For example, a video website that has a play button on it which says 'click to play a free video', but an invisible iFrame has been placed on top of the page and lined up exactly with the play button. The consumer tries to click on the play button but instead has actually clicked on the invisible iFrame and is directed to another site. In essence, the consumer's click has been "hijacked".

In a PRS context, the consumer could be misled by being redirected to a website offering a PRS promotion, which may lead to a purchase under false pretences. In this example a compliant web promotion may be masked or obscured by something which attracts the consumer to click on a consent to charge icon or button without them fully understanding the potential costs.

Where a PRS promotion is linked to a promotion from another website, the link should be open and transparent, allowing consumers to make an informed choice. PRS promotions should clearly state what the service is, how it operates and, where possible, its cost, displaying relevant key information in a visible, legible and proximate format. Consumers should be fully aware as to what they are engaging in before any charging commences.

Likejacking

Likejacking is similar to clickjacking however it targets a consumers social media pages. It is similar because the consequences of any user's engagement with the 'like' function are not explained or clearly presented to them before its use. But unlike clickjacking the consequences may not be directly linked to a payment transaction. Instead other consumers are encouraged to pursue a link based on their contact's – potentially unknowing – endorsement. In certain cases, clicking on their contact's endorsement may result in them unintentionally 'liking' the same promotion and further

publicising it under false pretences. The deception is particularly effective and spreads virally due to the personal nature of the endorsement.

The 'liked' link may then take the consumer to a website containing a PRS promotion, often with inadequate transparency. Consumers are therefore engaging in a promotion based on a contact's supposed endorsement as well as marketing the promotion themselves, without their prior consent. Likejacking is thus capable of contravening Code requirements around fairness and consumer privacy, and may lead to an investigation into relevant PRS.

Providers must ensure that premium rate services do not cause the unreasonable invasion of consumers' privacy (see Rule 2.4.1 of the Code). This includes leveraging a consumer's network of contacts without their explicit and knowing consent. Any links to a consumer's network of social media contacts should only commence after specific, auditable evidence of consent to do so has been received by the provider. Independently verifiable records of consent should be made available to the PSA upon request.

Misleading banner ads, pop-ups and pop-unders

Banner ads, pop-ups and pop-unders aim to attract consumers to promotions, usually based on other websites. It is important that the full user experience is considered when establishing promotional material, especially that which is within the control of the service provider and the promotion at the point of sale. In most cases, where pricing and other key information is clearly stated, they are likely to be compliant.

However, when a banner ad, pop-up or pop-under establishes a particular expectation or provides an inducement that contradicts the real product or service offering on the PRS website (particularly where it leads to a website where pricing information is not clearly stated) problems may arise. The consumer might be misled in contravention of the Code requirements.

In some cases, banner, pop-up and pop-under advertisements promise high street vouchers in order to induce customers to follow their link. Whilst the subsequent website may be transparent in terms of price and other conditions, the consumer may consent to a charge in the mistaken belief s/he will receive high street vouchers as a result. In cases where a consumer has been induced in a misleading fashion, a compliant landing page may not fully correct or remedy the impact of that inducement.

Consistent with Rules 2.2.1 and 2.3.2 of the Code, all PRS promotions should be as open and transparent as possible and must not mislead, and thereby allow consumers to make an informed choice. Links to PRS promotions must therefore be open and transparent and not entice consumers under false pretences. PRS promotions must clearly state what the service offered is, how it operates and, where possible, its cost, displaying relevant key information in a visible, legible and proximate format.

Misleading search engine marketing and search engine optimisation

Search engine marketing (SEM) and search engine optimisation (SEO) both aim to improve a service provider's visibility in search engine results pages. Both are prominent and legitimate means for

service providers to market their products. However, misleading terms could be used to artificially boost search engine ranking.

Providers are expected to use key words or meta tags that are accurate descriptors of the service being offered and should not mislead consumers either about the cost or the nature of the service. For example, where the meta tag 'free' is used, then the free element of the service must be made abundantly clear. If none of the service being offered is free, or the free element is not made abundantly clear, then the service is likely to contravene the Code outcome of fairness. Any reference to a brand association or company to which the provider is not associated is also likely to be considered misleading if it confuses consumers about the nature of the service being offered. The service provider's own brand should be prominent and be displayed clearly as the operator of the service.

The PSA has also noticed examples of websites being compromised by PRS promotions. For example, a consumer enters a search term into a search engine that is completely unrelated to any PRS promotion. Having found the link they are looking for, the consumer clicks on the appropriate link only to be taken to a PRS promotion. Use of forced re-directs in this manner may contravene the Code and we will investigate where necessary.

Content locking

When a practice known as content locking or content unlocking is used, consumers are enticed into purchasing a product, often PRS, in order to access unrelated content. Consumers may be looking to download an app or a new film or access a particular offer (shopping vouchers for example), which is not made available until they go through a certain number of steps where charges might be incurred. In PRS terms, a consumer might for example be prompted to enter his or her mobile phone number in order to download a film or access shopping vouchers but in reality they are entering into a subscription-based quiz. Effectively consumers enter the quiz to access the 'locked' content.

Ransomware[1] is a particularly severe case of content locking where a consumer's browser is locked. The consumer is then invited to enter a survey to 'unlock' his or her browser, effectively being held to 'ransom' in the process. Completing the survey then enters the consumer into a PRS promotion and often the browser remains locked.

PRS promotions that garner consumer consent to engage in PRS in order to access unrelated content are likely to be considered misleading if the relationship between the service and unrelated locked content is not genuine. Any investigation would centre upon the transparency of the transaction and the fairness of charging a consumer for an unwanted third-party service in order to pay for access to the original content. Where such original content is not supplied, this may be considered an aggravating feature of the PRS marketing campaign managed by the service provider.

[1] Ransomware is a type of malware that restricts access to a computer system that it infects in some way, and demands that the user pay a ransom to the operators of the malware to remove the restriction.

Adware

Adware[2] involves the downloading of software that propagates advertising designed to generate revenue for the developer. In principle this can be compliant with the Code, but, at the time of writing, we had rarely seen occasions when it has been compliant. We have particular concerns as to where adware is contracted without informed consent and the control it grants to a developer to manipulate a consumer's browser.

If a provider cannot ensure the prevention of consumers contracting any adware through PRS promotions they may view, we recommend that the provider reconsiders promoting its service through these means. Indeed, data relating to sales trends and customer service trends may prompt internal investigations into particular consumer journeys or advertising campaigns with a view to intervening and remedying any issues, including potential breaches of the Code.

Unsolicited electronic communications

The PSA receives numerous complaints from consumers about PRS marketing that, they feel, encroaches on their privacy. This includes potentially unsolicited email marketing that may, in certain cases, contain malware.

As set out in Rule 2.4.1 of the Code, consumers have the right to privacy. In line with guidance from the Information Commissioner's Office, electronic marketing can only be sent to consumers if the consumer has consented to receive it or if there is an existing, clearly defined and direct customer relationship and the customer is provided, in each marketing communication, with an opportunity to opt out and does not do so. For more information on the PSA's expectations around the consumer's right to privacy, providers should see the Privacy Guidance.

[2] Adware, or advertising-supported software, is any software package that automatically renders advertisements in order to generate revenue for its author. The advertisements may be in the user interface of the software or on a screen presented to the user during the installation process.

Annex to Digital Marketing and Promotions Guidance: Direct Buy Marketing

This Annex provides information on Direct Buy Marketing, including its benefits and risks. It is intended to support providers of phone-paid services to comply with the Code of Practice when using Direct Buy Marketing, and to ensure that consumers are adequately protected from potential harm.

Information and Guidance on Affiliate Marketing, the other digital marketing technique most commonly used to advertise premium rate services, can be found here.

The Annex is structured as follows:

- Definition of Direct Buy Marketing
- The potential risks associated with using Direct Buy Marketing
- Targeting through Direct Buy Marketing
- Settings to reduce the risk of consumer harm when using Direct Buy Marketing
- Measures to control ad placement and ensure ads are targeted as intended
- Roles and responsibilities in the Direct Buy Marketing model
- Payment mechanisms.

Defining Direct Buy Marketing

Direct Buy Marketing is the direct placing of adverts via major online platforms. In this model, a provider can purchase and select the account and campaign settings themselves or use a third-party provider to develop and monitor their account and specific advertising campaigns. As one form of marketing, Direct Buy Marketing helps to ensure that advertising operates effectively using techniques such as targeting and exclusion. The way these techniques are used will vary slightly across different platforms. Google (including YouTube) is currently the most commonly used platform.

Direct Buy Marketing can target information about goods and services to consumers based on their geographical location, their search terms (using a keyword strategy), by mobile network operator (when the consumer is using a mobile data connection) and by device. Direct Buy Marketing gives the service provider significantly more control over the placement of advertising than other methods such as Affiliate Marketing. However, it does carry some risks.

With increased use of Direct Buy Marketing, the PSA saw increased prevalence of adverts for phone-paid services appearing in content likely to appeal to children. However, the PSA has since seen a significant reduction in the prevalence of advertising for phone-paid services appearing in children's content. This is in part a result of the PSA and industry working together to resolve this issue, as well as action on the part of providers to ensure that they are complying with the Code. For example, workshops organised by PSA, Google and mobile network operators.

The most commonly used method of Direct Buy Marketing is Google Ads, an engine that places ads on online platforms. Google Ads is split into two networks: the Google Search Network and the Google Display Network (GDN). Advertising on the search network means text ads are placed in search engine results. On the GDN, businesses place display ads on a network of sites across the internet.

What are the potential risks associated with using Direct Buy Marketing?

With the increased use of Direct Buy Marketing, the PSA saw an increase in the number of adverts from providers of phone-paid services appearing in videos on major platforms and apps that are likely to appeal to children. This led to a concern that because the consumer journey often has low levels of friction through to payment, some consumers, particularly children, are unknowingly engaging with phone-paid services.

For example, young children may be watching a children's video and click through to a purchase on a subsequent website that a banner links to, without understanding the cost implications (even if pricing information is clear) because they are attracted to a large, brightly coloured, and sometimes animated button.

This Guidance provides information on how providers can effectively use the tools available to use Direct Buy Marketing and reduce the risk of consumer harm.

Targeting through Direct Buy Marketing

Google Ads uses a range of techniques to promote products and services (including phone-paid services). These techniques include text-based ads, graphic display ads, YouTube video advertising and in-app mobile advertising. Google Ads charges the provider for each click on the ad, view of the YouTube video, or specifically in the context of phone-paid services, calls placed through the ad. The provider can set preferences in their account and at campaign level to specify the approach to charging.

Consumers can be targeted in different ways through Google Ads. This includes targeting:

- using the location of the consumer
- specific devices and mobile device users
- specific Google account users based on their interests and demographics (restriction by age is also possible)
- based on a user's previous engagement with similar products and services
- specific, listed locations based on a pre-approved list.

Using these techniques to target adverts helps to ensure that consumers are protected from the harm caused by inadvertent placement of advertising and means that products and services are tightly targeted.

There are different settings available which can be used to target and exclude groups of consumers, depending on the type of advertising and whether exclusions are made at the account or campaign level. You will find further information on these below.

Settings to reduce the risk of consumer harm when using Direct Buy Marketing

Account level settings

At the account level, it is possible to exclude websites or domains so that advertising content does not show on them. This is beneficial to phone-paid services providers as it helps to ensure that certain vulnerable groups of consumers, such as children, are excluded from seeing inappropriate ads. Account level exclusions mean that the specific website or domain exclusions apply across each of the different campaigns that a provider may have.

Account level exclusions prevent ads from showing on selected placements on the GDN and Google Search Network and override campaign level placement targeting. Key account level exclusions include:

- *Subdomains:* to successfully create an exclusion at the account level, it is critical to exclude the *www* from a web address. Excluding the www means that any subsite, subdomain or subpage will also be excluded, and so is an effective way of broadly excluding placements.
- *Country domains:* different country domains need to be excluded separately. For example, both example.co.uk and example.com would both need to be on the exclusion list.
- *Limits:* it is possible to enter up to 20 shared placement exclusion lists at a time and a total of 65,000 exclusions per list. Separate from your list, campaigns and group exclusions, it is also possible to enter 65,000 account-level placement exclusions per account. Lastly it is possible to enter 128,000 placement exclusions per ad group.

Campaign level settings

When setting up a new campaign on the GDN, a range of settings must be selected to optimise targeting specific to the campaign. The selected campaign settings will apply to all ads within the same campaign.

Further information on each of these settings is outlined below.

- *Networks:* the networks setting determines where the ad will appear, based on campaign type. There are options for ads to appear on Google search sites and non-Google search sites.
- *Devices:* Campaigns target a range of devices, including desktops, tablets, and mobile devices. It is possible to customise ads for different types of device.
- *Locations and languages:* campaign ads will appear in selected geographic locations and/or to customers whose browser language setting matches the providers target language setting.
- *Additional settings:* Adwords automatically show ads when they are more likely to get clicks and conversions, but it is possible to manually set the timing of ad displays so that they are shown more evenly throughout a day, and to schedule certain days or hours in which ads will show.

It is recommended that phone-paid service providers take steps across each of these campaign and account level settings to ensure that adverts are targeted appropriately, and exclusions are in place that ensure practices are legitimate and able to satisfy the outcomes of the Code.

Smart Display Campaigns

A smart display campaign is powered by Google's machine learning. It shows ads in a range of formats across the GDN, using different tools to optimise conversions. For example:

- *automated optimisation* increasingly shows ads where they are more likely to get conversions. This is achieved through historical data and campaign results.
- *automated ad creation* combines the base information that a provider enters at the start of a campaign, such as headlines, descriptions and images, and selects the best combination of information to create ads. At the same time the system collects information about what is working well, to optimise the campaign.

- *automated bidding* is where the smart campaign bids most aggressively when performance data suggests the highest likelihood of conversions and less often when data suggests there is a lower likelihood of conversions.

Adwords exclusions also apply to smart display campaigns. This means that both account-level ad placement exclusions and site category and content exclusions can be applied to prevent ads from showing on specific sites or appearing as part of specific searches. This means the campaign is optimised by machine learning, but that the advertiser still can take steps to prevent the ad from appearing on specific sites.

Measures to control ad placement

Further information on ad exclusion techniques is outlined below. Activity should be undertaken in each of these areas to ensure that adverts are targeted appropriately.

Negative Keywords

A negative keyword is a specific word that helps to prevent ads from being displayed to consumers who are unlikely to click the ad or for whom the ad is not suitable. Negative keywords prevent the ad from appearing in a consumer's search, if their search contains the exact words that have been explicitly excluded.

It is possible that ads may still appear in a consumer's search, because excluded keywords may not be as precise as they are in the search. For example, if the negative key words 'kids show' are excluded, the ad may still show on pages that contain the terms 'kids cartoon' or 'shows for children'. Further information on negative Keywords can be found here.

To prevent ads from appearing in content that they were intended to be excluded from, it's necessary to develop a precise match negative keyword list which contains various permutations of the words intended to be excluded.

It is important to note the following:

- The system can apply a list of up to 10,000 negative keyword terms per campaign. If there are more than 5,000 keywords across the ad group, campaign or shared list, the system will not be able to apply all the negative keywords in the list.
- At the time of publication, it was not possible to exclude phrases. However, an alternative approach identified by Google is to separate the words in phrases and add each word as a separate keyword.
- It can take up to 48 hours (occasionally longer) for new YouTube content to be classified. During the period in which content is unclassified, any keyword strategy in place will not apply to new content until it has been classified. To avoid ads being inadvertently targeted to unintended audiences (such as children), the PSA recommends that content 'Not Yet Rated' should be excluded from advertising campaigns
- Negative keywords cannot be used for Smart Display campaigns (more information on Smart Campaigns can be found here)

There are also Google Adwords policy restrictions to be aware of. Further information on these can be found here.

URL blocking

URL blocking means that ads won't be placed on specific listed webpages. The exact URL that is intended to be blocked must be listed for this exclusion technique to be effective. URL blocking on YouTube can be done by channel at account and campaign level, but otherwise must be done by specific video.

Topic and category exclusion (note that at the time of publication this was only available on iOS)

This excludes the ad from appearing on pages about specific topics. For example, apps purchased through Apple or Google Play can be listed by category, and it's possible to exclude an ad from appearing in any search for an app that is listed within that category. At the time of publication, there was a negative app category available for children only on Apple.

YouTube content can also be excluded based on its classification.

Therefore, the recommended approach is to only allow ads to show on content that has been classified. This will prevent ads from appearing in unintended and unsuitable content places.
The approaches outlined above are supplementary. It is recommended that activity is undertaken across multiple exclusion techniques to ensure effectiveness and support accurate and appropriate targeting of ads.

Using a range of techniques will help to ensure that ads do not inadvertently appear in children's content and will prevent consumer harm. The exclusion topics, keywords, apps and URLs should be reviewed regularly to ensure that the approach adopted continues to be effective.

Topics and interest category exclusions can be made at campaign level.

Roles and responsibilities in Direct Buy Marketing

The Code of Practice requires network operators and Level 1 providers to undertake effective due diligence in contracting with any party that forms part of the value chain in delivering phone-paid services to consumers. In addition, both Level 1 and L2 providers, and network operators, are required to carry out a risk assessment on any party they contract with in respect of the promotion, marketing and content of the phone-paid services they provide to consumers.

Network operators and all providers are required to identify and manage risks, both prior to contracting and on an on-going basis throughout the contractual relationship. In the Direct Buy Marketing model, the Level 2 provider has responsibility for AdWords and is required to retain evidence of the AdWords exclusions in place. For example, information on the negative keywords and blocking in place.

The Level 1 provider is required to assess the risks of contracting with any other party, such as Level 2 providers, and to carry out reasonable monitoring of any provider that they contract with.

Level 1 providers should audit their Level 2 partners to assess the effectiveness of their control methods for Direct Buy Marketing and keep clear records of these audits. This should include a review of the AdWord exclusions that their Level 2 partners have in place to ensure the measures

taken to control ad placement are operating effectively. Taking these steps will help to ensure that the required Due Diligence and Risk Assessment and Control measures are in place and maintained.

These expectations apply to all forms of contractual relationship across the value chain but vary depending on which parties in the value chain the relationship is between. Providers are advised to review and comply with the Due Diligence and Risk Assessment and Control Guidance which provides more detailed information on the expectations and requirements.

Providers must also consider the range of risks associated with different clients and the services they provide and put systems in place to assess and manage the level of risk posed by a client and/or their service(s), with a focus on non-compliance with the Code and/or the law or causing consumer harm. This applies to all parties across the value chain.

Providers must make a proper assessment of the likely issues that would arise if incidents were to occur and take proportionate steps to minimise the likelihood of such issues resulting in consumer harm.