GENERAL GUIDANCE NOTE

Digital marketing and promotions

1. What is digital marketing and what problems may arise?

1.1 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, driving innovation and allowing consumers to engage with premium rate services (PRS) without causing harm or undue harm.

1.2 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, PhonepayPlus has seen instances where consumers have been misled by marketing using these techniques in the past.

1.3 Examples of practices which are always misleading:

- Typosquatting
- Clickjacking
- Likejacking
- Content locking

This is not an exhaustive list. The market is constantly evolving and while PhonepayPlus 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 bad practices can be found in the Annex to this Guidance.

1.4 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. For further assistance on controlling risk when using affiliate marketers please read part 10 of the 'Promoting premium rate services' Guidance[1].

1.5 Our principal concerns relate to three outcomes in the PhonepayPlus Code of Practice (the 'Code'): transparency, fairness and privacy.

[1] http://www.phonepayplus.org.uk/~/media/Files/13th-Code-of-Practice/Guidance-and-Compliance/Promoting-PRS_Oct_15v2.pdf

- 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. The sending of unsolicited electronic communications (spam) is unlawful. Any promotional material must be delivered appropriately and with the consumers consent, which must be knowingly given and clearly identifiable.

1.6 Businesses, advertisers and relevant trade bodies, such as the Internet Advertising Bureau (IAB), 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 PRS providers consider advice and support offered through such third parties[2].

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

2.1 PRS 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.

2.2 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 PRS provider regardless of whether this activity is sub-contracted to a third party such as an affiliate marketer. So if an affiliate marketers activities lead to a breach of the Code in relation to a PRS service, then a Tribunal will generally hold the PRS 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 above in an attempt to inflate their revenues by engaging consumers in services without their clear understanding and consent.

2.3 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 PhonepayPlus 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.

[2] The Internet Advertising Bureau website is www.iabuk.net

2.4 PhonepayPlus expects PRS providers to take account of PhonepayPlus' previous Guidance on Due Diligence and Risk Assessment and Control (DDRAC) on Clients. In particular, PRS providers should undertake effective due diligence on any affiliate marketer that they are seeking to engage. As stated in paragraph 2.1 of the Guidance on Due Diligence and Risk Assessment and Control on Clients, 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 in addition to ongoing DDRAC considerations already set out in Guidance elsewhere (this 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):

a) Companies checks;
b) Reputational checks through Google, blogs, AV vendors, Level 1 providers etc.;
c) How established the affiliate marketer is;
d) 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;
e) Whether the affiliate marketer is aware of and committed to 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;
f) How the affiliate marketer sources its traffic. For example, does it source its traffic from file-sharing websites (this will likely result in increased risk);
g) If the affiliate marketer sub-contracts with other affiliate marketers in doing so (which will amplify any risk) and how it sources and vets individual affiliates;
h) Whether the affiliate marketer is willing to explain where and in what terms it plans to place your advertising;
i) Using traffic monitoring using tools such as Alexa or SimilarWeb to understand how an affiliate generates traffic;
j) The level and sophistication of the tracking technologies the affiliate uses;
k) Whether the marketer in question has fraud detection systems and monitoring tools is place;
l) Whether the affiliate marketer is prepared to run its service on a trial basis.

2.5 In addition, PhonepayPlus expects PRS providers throughout the value-chain to:

a) Set clear expectations for their affiliate marketers around Code compliance and obtain a clear commitment to this end as part of any contract signed. Expectations should include (but are not limited to):
    i. Price and other key information should be clearly stated;
    ii. Any marketing be directly related to the PRS offering i.e. not unrelated and misleading;

b) That affiliates will not engage in any of the misleading practices listed above or any other such misleading practices.

c) 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.

d) 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 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. It can be found at: http://www.iabuk.net/resources/standards-and-guidelines/conducting-affiliate-audits-best-practice.

e) Make it clear to affiliate marketers (and reflect this in the contract) that any failure to comply with the expectations set will result in suspension of payments.

f) 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 PhonepayPlus upon request.

2.6 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):

a) Check which affiliates or your client contracts with, identifying any affiliate that might pose a significant risk;

b) Ensure your client has appropriate contractual arrangements and risk control processes in place to deal with affiliate marketing and misleading digital marketing more generally;

c) Undertake thorough and frequent checks to ensure your client's promotional material meets the outcomes set out in the Code;

d) Monitor activity for abnormal service behaviour on an ongoing basis;

e) Generally ensure that your 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 [3]

[3] http://www.phonepayplus.org.uk/~/media/Files/13th-Code-of-Practice/Guidance-and-Compliance/Due-diligence-risk-assessment-and-control.pdf

ANNEX

EXAMPLES OF BAD PRACTICE

The following are detailed examples of non-compliant practices that should be avoided:

1 Typosquatting

1.1 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 is done with the intention of redirecting consumers who mistype or click on mistyped links away from their intended destination. Consumers are then led to a website that is designed in a confusingly similar manner to the website that they were originally searching for.

1.2 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 looks like his or her intended destination but contains a PRS promotion. The consumer may pursue the promotion based on its pertained association with a trusted brand.

1.3 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.

2 Clickjacking

2.1 ‘Clickjacking’ is a malicious technique of tricking 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 disguised link (the link may be hidden using transparent IFrames[4]), 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 website that has a button on it that says "click here for a free iPod" however, an invisible IFrame has been placed on top of the page with a consumers email account, and lined up exactly the "delete all messages" button directly on top of the "free iPod" button. The consumer tries to click on the "free iPod" button but instead actually clicked on the invisible "delete all messages" button. In essence, the consumers click has been "hijacked".

[4] An IFrame (Inline Frame) is an HTML document embedded inside another HTML document on a website. The IFrame HTML element is often used to insert content from another source, such as an advertisement, into a Web page.

2.2 In a PRS context, the consumer will be misled into redirecting to a website offering a PRS promotion, which may lead to a purchase under false pretences. Another example would be of a website obscuring compliant pricing information, attracting the consumer to click on a consent to charge icon or button without fully understanding the potential costs. These are highly likely to be in breach of either Rule 2.3.2 or 2.2.1 of the Code.

2.3 As set out in Rule 2.3.2 of the Code, providers should not mislead consumers. This includes linking to a website offering PRS without the consumer's prior knowledge.

2.4 Consistent with Rule 2.2.1, all PRS promotions should be as open and transparent as possible, allowing consumers to make an informed choice.

2.5 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 – we believe that consumers should not be misled into visiting websites that they did not intend to. 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.

3 Likejacking

3.1 Likejacking is a form of clickjacking that targets a consumers social media pages. 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 works in the same way as clickjacking using a transparent IFrame to disguise a link.

3.2 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 highly likely to be breach the Code's requirements around fairness and consumer privacy.

3.3 As set out in Rule 2.3.2 of the Code, providers should not mislead consumers. Links to PRS promotions must be open and transparent, allowing consumers to make an informed choice. Promotions must clearly state what the service offered is, how it operates and its cost, displaying relevant key information in a visible, legible and proximate format. Ultimately consumers should be in no doubt as to what they are engaging in before any charging commences.

3.4 As set out in Rule 2.4.1 of the Code, providers "must ensure that premium rate services do not cause the unreasonable invasion of consumers' privacy." 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 PhonepayPlus upon request.

4 Misleading banner ads, pop-ups and pop-unders

4.1 Banner ads, pop-ups and pop-unders aim to attract consumers to promotions, usually based on other websites. In most cases, where pricing and other key information is clearly stated, they are likely to be compliant.

4.2 However, when a banner ad, pop-up or pop-under leads to a website where pricing information is not clearly stated, and thus the consumer might be misled, the provider is highly likely to be found in breach of the Code.

4.3 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 is unlikely to be accepted as a defence by the Tribunal.

4.4 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. 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.

5 Misleading search engine marketing and search engine optimisation

5.1 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 PRS providers to market their products. However, misleading terms could be used to artificially boost search engine ranking. This practice is highly likely to be found misleading by the Tribunal.

5.2 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, all or at least the majority of services being promoted should be free. If none or only a minority of services being offered are free, a PhonepayPlus Tribunal is highly likely to find such practice in breach of the Code. Any reference to a brand 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.

5.3 PhonepayPlus 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. This is clearly a breach of any expectation PhonepayPlus has around digital marketing.

6 Content lockers

6.1 In many cases, the practices listed above all lead the consumer to interact with a service through several steps. Content locking is often seen in conjunction with misleading digital marketing. These include clickjacking, likejacking and misleading SEM/SEO.

6.2 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.

6.3 Ransomware[5] 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.

6.4 As set out in Rule 2.3.2 of the Code, providers should not mislead consumers. PRS promotions that garner consumer consent to engage in PRS in order to access unrelated content are likely to be considered misleading. Content locking is almost certain to be considered in breach of the Code if the consumer is not made fully aware of the cost of accessing the unrelated content and/or the content is not delivered.

[5] 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

7 Adware

7.1 Adware[6] 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.

7.2 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, if the consumer journey to a particular promotion were found misleading or result in an unwanted invasion of consumer privacy, it is likely to be in breach of the Code.

8 Unsolicited electronic communications (Spam)

8.1 PhonepayPlus 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.

8.2 By definition, spam, even where it is not misleading in terms of content, is likely to be considered in breach of the Code as outlined above. For more information on PhonepayPlus' expectations around the consumer's right to privacy, providers should see the General Guidance Note on Privacy[7].

8.3 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 PhonepayPlus' expectations around the consumer's right to privacy, providers should see the General Note on Privacy.

[6] 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.
[7] http://www.phonepayplus.org.uk/~/media/Files/13th-Code-of-Practice/Guidance-and-Compliance/Privacy.pdf