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) as a payment method.

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, and 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 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 user's 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".

1.4 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 practices, including those mentioned above, that may cause a breach of the Code can be found in the Annex to this Guidance.

1.5 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[1].

1.6 When managing any digital marketing campaign, PRS providers should address potential risks by actively seeking to meet outcomes in the PhonepayPlus Code of Practice (the 'Code'). In particular, PRS 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.

1.7 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].

[1] http://www.phonepayplus.org.uk/~/media/Files/13th-Code-of-Practice/Guidance-and-Compliance/Promoting-PRS_Oct_15v2.pdf
[2] The Internet Advertising Bureau website is www.iabuk.net

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 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.

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.

2.4 PhonepayPlus expects PRS providers to take account of PhonepayPlus' Guidance on Due Diligence and Risk Assessment and Control (DDRAC)[3] 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 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):

a) Companies checks;
b) Reputational checks through app stores, blogs, AV vendors, Level 1 providers etc.;

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

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 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;
f) 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;
g) 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;
h) 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;
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 where funds are capped until the relationship is fully established.

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.
b) Ensure 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 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. 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 or forfeiture 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) 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;

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

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

d) Monitoring activity for abnormal service behaviour on an ongoing basis and taking action upon it;

e) 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[4].

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

ANNEX

EXAMPLES OF PRACTICES THAT MAY CAUSE A CODE BREACH

These examples are provided to equip PRS 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, PRS providers will improve compliance standards across the PRS market.

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 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.

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 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.

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.

1.4 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.

2 Clickjacking

2.1 ‘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 " however, 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".

2.2 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.

2.3 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.

3 Likejacking

3.1 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.

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 capable of contravening Code requirements around fairness and consumer privacy, and may lead to an investigation into relevant PRS.

3.3 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 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. It is important that the full user experience is considered when establishing promotional material, especially that which is within the control of the PRS 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.

4.2 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.

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 may not fully correct or remedy the impact of that inducement.

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. 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.

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.

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, 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 PRS provider's own brand should be prominent and be displayed clearly as the operator of the service.

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. Use of forced re-directs in this manner may contravene the Code and we will investigate where necessary.

6 Content locking

6.1 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.

6.2 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 and often the browser remains locked.

6.3 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 PRS provider.

[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, 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.

8 Unsolicited electronic communications

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 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 Guidance Note on Privacy[7].

[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