Consultation on Guidance on digital marketing and promotions

A Final Statement following PhonepayPlus' Consultation

Publication Date: 19 November 2013

Table of Contents

Introduction

PhonepayPlus issued a consultation on digital marketing practices and promotions on 16 May 2013. The consultation was open to responses for six weeks, closing on 27 June 2013. The consultation received 16 responses from a variety of providers throughout the value-chain and other interested stakeholders. These can be found on the PhonepayPlus website.

PhonepayPlus first issued the consultation in response to increasing consumer complaints about the digital marketing of premium rate services (PRS). Prior to publication, we estimated that 40% of complaints we receive were directly related to the digital marketing of PRS. This has since declined to around 20%. We believe the reasons for the decline in complaint numbers are twofold: first the publication of draft Guidance raised awareness among PRS providers of our concerns and, second, the action taken by the Tribunal against non-complaint providers has underlined the potential consumer harm caused by misleading digital marketing.

Despite the drop in complaints, we still receive around 200 complaints per month relating to the digital marketing of PRS. We remain concerned that this number could rise quickly in a fast moving marketplace.

The original consultation outlined seven potentially misleading practices that we had identified in the context of the online promotion of PRS. These were typosquatting; clickjacking; likejacking; banner ads, pop-ups and pop-unders; search engine marketing (SEM) and search engine optimisation (SEO); content-lockers and spam.

The consultation outlined why we believe that, in certain circumstances, these practices are likely to be found in breach of the Code by a Tribunal. The consultation then detailed proposed Guidance on how PRS providers can help to ensure consumers are protected from potential harm and that their services can be compliant with the Code.

The consultation posed 11 questions to respondents. These asked for respondents' views of our proposed approach to misleading digital marketing, the seven practices we identified and our proposals to help address them, and our understanding of affiliate marketing and associated recommendations.

In general, responses were supportive of our approach to and understanding of the misleading digital marketing practices we identified in the consultation. However, respondents raised issues where they felt the Guidance could be clearer as well as areas that they felt the Guidance would not address the problems identified. In particular, respondents raised four issues that they felt required clarification or further consideration. These are (in alphabetical order):

- Adware
- Affiliate registration
- Due Diligence Risk Assessment and Control
- Tracking and monitoring of affiliate traffic

We have tried to address these concerns in this document and Guidance. We do not believe that respondents' comments render our proposed Guidance invalid but rather strengthens it by ensuring the Guidance achieves consumer protection and the outcomes outlined in the

Code. We have therefore updated the draft Guidance taking account of respondents' views and refining it where appropriate.

This document sets out our understanding of the responses we received to the consultation and any changes to the draft Guidance that we have considered as a result. Finally, the document includes PhonepayPlus' finalised Guidance on Digital Marketing Practices and Promotions in support of the Code of Practice.

The finalised Guidance differs from the draft Guidance in that it:

- Addresses industry concerns around adware
- Clarifies our position on tracking and monitoring
- Suggests a number of due diligence, risk assessment and control measures that both Level 1s and Level 2s can employ before and whilst contracting with various affiliate marketing partners.

Summary of Responses and Conclusions

In general, responses were supportive of our understanding of the misleading digital marketing practices we identified in the consultation. Comments received in response to Question 1 were general in nature. In this document, we therefore consider any specific points received in response to Question 1 as part of our consideration of responses to Questions 2 to 11.

Following consultation responses and wider feedback we have also sought to ensure that the Guidance is as clear as possible. In doing so, we have clarified any language that could have been clearer. Where this does not change the meaning of the original text, we have not drawn attention to the changes.

Question 2: Do you agree with our consideration of typosquatting and proposed expectation? If not, why not?

All substantive responses to Question 2 were in broad support of our assessment of typosquatting and related guidance. Remote Games noted that purchasing domain names to collect misspellings was common and not in itself misleading. We agree. As stated in the draft Guidance, typosquatting leads consumers "to a website that is designed in a confusingly similar manner to the website that they were originally searching for." Thus it is the registering and use of misspelt domain names in conjunction with confusingly designed websites that is highly likely to be considered in breach of the Code. We therefore propose to leave the Guidance on typosquatting as originally presented in the consultation.

Question 3: Do you agree with our consideration of clickjacking and our proposed expectations? If not, why not?

In general, responses supported PhonepayPlus' description of clickjacking and our proposed expectations. AIME, however, noted that the proposed Guidance on digital marketing goes beyond previous Guidance in recommending that promotions that do not carry the payment mechanism should carry all pricing information.

The current Guidance on pricing and promotional material states that "pricing information will need to be easy to locate within a promotion (i.e. close to the access code for the PRS itself), easy to read once it is located and easy to understand for the reader (i.e. unlikely to cause confusion)." We appreciate this is subtly different from Paragraph 3.5 in the draft Guidance.

However, given the nature of the consumer journey online, we believe that promotional material should endeavour to include pricing information as far as is possible. Therefore, we propose to insert the clause 'where possible' into the Guidance.

AIME also noted that the focus of the Guidance around clickjacking should be on not misleading the consumer. We agree that fairness is a key Code outcome but we feel that this is adequately reflected in the Guidance already.

Given responses received to Question 3, PhonepayPlus proposes to amend Paragraphs 3.3, 3.4 and 3.5 as such:

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

Question 4: Do you agree with our consideration of likejacking and our proposed expectations? If not, why not?

The majority of respondents agreed with our description of likejacking and draft Guidance, underlining PhonepayPlus' point that no service should leverage a consumer's network of contacts without their explicit and knowing consent. However there were two points raised by respondents that were worthy of further consideration.

AIME commented that we should make a clear distinction between commercial terms and conditions and our Guidance. Given that the draft Guidance makes no mention of any social media platform – Facebook was merely mentioned in the consideration – we do not propose to change it in this regard.

The other issue that arose out of responses was how a provider would audit whether a 'like' was legitimate or not. The draft Guidance did not intend to prohibit genuine endorsements on social media platforms. However, as raised by AIME, it can be difficult to ascertain whether an endorsement is genuine or not.

While we do not know of a technical solution to this problem, in our experience, this is usually fairly clear. Such endorsements tend to be fanciful, too good to be true or not in keeping with the individual's other posts.

Question 5: Do you agree with PhonepayPlus' consideration of banner ads, pop-ups and pop-unders and our expectations around them? If not, why not?

We received two substantive comments in response to question 5. In relation to Paragraph 5.3, it was noted that the draft Guidance should clearly state that if an initial inducement is misleading, a breach will likely have occurred even if the subsequent website is compliant. To this end, we propose to change Paragraph 5.3 as follows:

> 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.*

The second comment, received from both AIME and an anonymous respondent, was that Paragraph 5.4 referred to Rule 2.2.1 of the Code relating to transparency and not Rule 2.3.2 around fairness. We think that both transparency and fairness are equally important in this regard and have therefore decided to add reference to Rule 2.3.2 in Paragraph 5.4. In addition, we have reflected comments received in response to Question 3 about cost in Paragraph 5.4. The Paragraph now reads:

> 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.

Question 6: Do you agree with PhonepayPlus' definition of SEM and SEO and our expectations around them? If not, why not?

The majority of respondents agreed with our proposals. Two issues of note were raised by respondents. One point raised by Mobile Broadband Group and Remote Games was that the wording in Paragraph 6.2 of the draft Guidance would find brands adopting a rival's keywords or metatags to capture consumers searching for a rival brand misleading – this practice is permitted by Google.

This was not our intention. To clarify, the emphasis in the final sentence of Paragraph 6.2 is on the latter half of the sentence i.e. the use of adwords associated with other brands should be compliant as long as it is not used in a confusing manner.

The other example cited by Remote Games would not be covered by this Paragraph either. In the example cited by Remote Games, a consumer searches for football clips and is taken to a site where he or she can watch such clips. This may then lead the consumer to see a PRS promotion as part of the website s/he is viewing. However, as long as the consumer is not misled into the PRS service, the use of SEM and SEO in this particular case is not misleading. We therefore do not propose to change Paragraph 6.2.

Question 7: Do you agree with our consideration of content locking practices and our expectations around them? If not, why not?

Responses were in general agreement with our assessment of content locking. Following publication of the consultation, PhonepayPlus became aware of a severe form of content locking known as ransomware that required urgent remedy through ten Emergency procedures. We therefore make reference to ransomware in Section 7 of the Guidance by inserting the following:

> Ransomware is a particularly severe case of content locking or malware 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.

AIME and Remote Games noted that our consideration of content locking suggested that it would always be considered misleading in a PRS context. This was not our intention. Content locking can be legitimate if the provision of unrelated content is clear and transparent, is straightforward to access and delivery is timely.

However, we have not yet seen the legitimate use of content locking in the context of PRS; where we have come across content locking in a PRS context, the consumer has been misled into entering a survey and the content has never ultimately been delivered. To clarify this point, we intend to change Paragraph 7.4 as follows:

> 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 ~~highly~~ likely to be considered misleading.~~, especially where the~~ *Content locking is almost certain to be considered in breach of the Code if* a consumer is not made fully aware of the cost of accessing the unrelated content and/or the content is not delivered.

Question 8: Do you agree with PhonepayPlus' consideration of spam and our related expectations? If not, why not?

Responses were broadly supportive of our consideration and proposals. The Information Commissioner's Office (ICO) noted that email marketing can only be lawfully be sent to individuals where the individual has consented, or where an organisation can meet the 'soft opt in' criteria set out in their guidance.

Therefore the recommendation we set out to record consent is beyond the scope of PECR. In light of this comment, we propose to amend Paragraph 9.3 of the Guidance:

> 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 ~~there is explicit and auditable consent~~ *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 and Consent to Charge.

Question 9: Are there any other potentially misleading digital marketing practices that we have not identified?

In response to question 9, a number of providers including AIME, Boungirono, Goverifyit and Zamano, mentioned adware and several asked for PhonepayPlus' view on it. Adware is, broadly speaking, software that displays advertising and is often embedded within another

program. It can be legitimate and is, indeed, used by blue chip brands. Advertising may be imbedded within a software application for example Skype. Another example might be the download of a Nectar search toolbar that prompts consumers with offers and promotions related to their internet usage.

However, the use of adware in a PRS context is not always legitimate. In fact, our monitoring has rarely identified the use of adware by PRS providers that would be considered compliant. Having responded to calls within consultation responses and conducted extensive research into the subject, the manner in which a consumer may download advertising software is an issue of real concern.

In a number of cases, we have identified that a consumer may unknowingly or inadvertently download such software that leads to unwanted advertising. A recent example noticed by PhonepayPlus involved the appearance of a dialogue box on consumers' browser that alerted them that they needed to upgrade their media player. Designed in a confusingly similar fashion to a legitimate media player (in this case Adobe Flash player), the consumer is then duped into downloading both an upgrade of the player as well as a form of adware in the process.

Here the consumer has been misled into downloading adware that was bundled together with an upgrade to his or her media player. In the process of downloading both, the consumer may be presented with various terms and conditions, some of which consent to allowing the developer to alter the consumer's browser and homepage. In this case, the consumer ended up installing new toolbars injected with advertising in the form of fictitious emails as well as contracting advertising injected[1] into his or her homepage and/or the page that s/he was viewing, promoting games, quizzes and other products. As such, the unintended consequence of a consumer upgrading their media player is to cede control of their browser and allow a developer to change the appearance of sites they view.

In other instances, we have identified other worrying forms of advertising propagated by installed adware. For example, we have noticed advertising inserted into text on well-known websites.

Not only is a consumer misled into downloading something they perhaps would not have chosen to, there is also an issue about consent to marketing. Whilst there may be evidence of consent to marketing, whether this consent is clearly informed and understood is highly questionable.

The second major issue of concern is that the downloaded software can give the developer significant control over what the consumer sees. Not only does this allow the developer to potentially manipulate the consumer's browser but it also presents significant risk to the advertiser. For example, the software may intentionally obscure important terms and conditions, including pricing, thereby duping a consumer into a service under false pretences. This would clearly be in breach of the transparency and pricing outcome in the Code. Another example may be where unwanted advertising appears as part of a legitimate website, without that website's permission. We also acknowledge the point made by AIME and Zamano that the developer's control of the consumer's browser presents monitoring

[1] Associate Professor Ben Edleman of Harvard Business School refers to this type of advertising as 'injectors'.

challenges but we would suggest that this merely underlines the risk associated with adware.

Zamano also asked for our view on search term redirecting. We see this as a form of adware that is likely to raise the same concerns as other forms of adware.

Given the concerns outlined, we propose to add the following guidance on adware:

> Adware 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 situations 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 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 to be found misleading or result in an unwanted invasion of consumer privacy, it is likely to be in breach of the Code.

We are conscious that the market is constantly evolving and new threats are continually emerging. An example would be the surfacing of ransomware in the PRS context, which, through the Emergency procedure, we were able to work with industry to ensure that potential consumer harm was negated.

Whilst PhonepayPlus will endeavour to maintain an up-to-date list of misleading practices that we have identified through guidance, compliance advice, notifications for example, we acknowledge that we will not always be able to identify every single misleading practice in the marketplace. We therefore urge providers to consider how various practices that they may have identified meet the outcomes set out in the Code and welcome any assistance in communicating these practices to the industry.

To clarify this position in the Guidance, we intend to amend the following sentence to the Executive Summary:

> **What is the purpose of this Guidance?**
>
> To ensure consumers are protected from potential harm and to assist all companies marketing PRS in the digital space to better understand and comply with the Code of Practice (the Code). It sets out PhonepayPlus' expectations related to compliant digital marketing and ~~details~~ *provides some examples of* what might be considered misleading. This Guidance supports previous work, the *General Guidance on Promotions and Promotional Material*, and builds on the '*Misleading digital marketing of premium rate services'* compliance update issued in February 2012. Before reading this Guidance, providers should familiarise themselves with the expectations set out in both of those publications.

And add the following to Paragraph 1.2:

> 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 emerging practices are likely to meet the outcomes set out in the Code. The fact that an unfair practice is not listed in this Guidance is unlikely to be treated by the Tribunal as a defence to an alleged breach of the Code.

Question 10: Do you agree with our illustrative representation of affiliate marketing? If not, why not?

There was general agreement with our representation of affiliate marketing. Three responses noted that the diagram did not take account of the complexity of affiliate marketing. Although we did note this in the consideration, we again note this here. However, as the diagram did not appear in the draft Guidance document nor the final Guidance, we do not intend to make any changes to it.

Question 11: Do you agree with our consideration of affiliate marketing and our expectations? If not, why not?

Many of the responses received devoted significant attention to question 11 around the issue of affiliate marketing. While a large proportion of responses were supportive, the issue of affiliate marketing was perhaps the most contentious.

The Internet Advertising Bureau, for example, felt that our consideration of affiliate marketing overplayed the unethical behaviour of affiliate marketers and suggested that the mainstream were committed to good practice. We agree; it was never our intention to tarnish the affiliate marketing industry.

In the majority of cases, the PRS industry uses affiliate marketing in a legitimate and effective manner, allowing consumers to engage with their services in a transparent and fair way. However, as outlined, we have noticed that a significant proportion of consumer complaints we receive are directly related to the digital marketing of PRS. Under the Code, providers are responsible for the promotion of their services. For the avoidance of doubt, we therefore intend to add the following sentence to the Guidance's Executive Summary:

> Providers must also ensure that they have adequate control over marketing done on their behalf by third parties, such as affiliate marketers. *A Tribunal is highly unlikely to accept arguments that it was the actions of an affiliate that was responsible for a breach of the Code as justification for avoiding liability under the Code for that breach, although such action may be taken into account in terms of mitigation.*

A number of responses questioned why affiliate marketers were not required to register with PhonepayPlus. Those respondents argued that bringing affiliate marketers under PhonepayPlus' regulatory remit would discourage malpractice among affiliates and would thus further ensure consumer protection.

While we acknowledge this argument, we do not believe that affiliate marketers can be brought under PhonepayPlus' regulation as they are not deemed to be providers of premium rate services under the Communications Act 2003 (the Act).

Furthermore, there is no evidence that the Code cannot deal with the issue of PRS affiliate marketing; a number of adjudications have been brought and upheld against Level 2 providers in terms of their responsibilities in this area in the last 18 months. Therefore, at this juncture, we do not see the need for a change in the law to enable affiliate marketers to be regulated by PhonepayPlus.

Indeed, AIME noted that affiliate registration would add considerable administrative cost for arguably little benefit; as is already detailed in the Code, Level 2s would still hold responsibility for their marketing regardless.

Other suggestions included a black list of rogue affiliates networks or a gold list of sanctioned or approved networks. We do not believe PhonepayPlus can publish a list of rogue affiliate networks as there are legal difficulties in publishing a list of affiliates involved in enforcement cases where they are not the party subject to regulatory proceedings.

At this juncture, we do not see the overriding merits of producing a list of approved networks either. This would potentially limit the choice of networks available to PRS providers, artificially distort the market and may create unnecessary confusion for a Tribunal when considering potential Code breaches involving so called ‘approved networks’. In addition, it is not our intention for PhonepayPlus to be perceived as directly or indirectly endorsing the services of any particular affiliate marketers.

In terms of monitoring affiliate campaigns, a number of respondents argued that affiliate marketers often presented compliant promotional material to providers but subsequently switched it for non-compliant materials once live. We are thus of the opinion that ongoing, systematic monitoring is in the interest of the provider to ensure that its affiliate partners are acting in its interest.

We acknowledge that this is no ‘silver bullet’ solution; monitoring by its nature is reactive and can be resource intensive. However, we do believe that monitoring is an effective means to contribute to ensuring a provider’s marketing material that is handled by affiliates is compliant. Indeed, particular attention should be given not just to unexplained spikes in traffic but all abnormal activity and traffic.

In the draft Guidance, we also noted that providers should closely monitor traffic from an affiliate network that has been previously associated with a breach of the Code in the past. Following feedback, we are of the opinion that this could be strengthened; if an affiliate network has been associated with a breach, a provider should strongly consider its relationship with this network rather than more closely monitoring traffic. As such, we have removed this from Paragraph 9.5 of the draft Guidance and placed this recommendation in a specific section on due diligence risk assessment and control (DDRAC).

Our initial expectations around tracking were met with a degree of resistance. A number of respondents argued that it was unrealistic and technically challenging to expect Level 2 providers to be able to record and retrospectively recreate all consumer journeys. Respondents also argued that there are currently no tools available to do this.

We have found some tools that could assist providers in doing this but acknowledge that they are not widely available. Our experience to date has been that US-based Scrubkit and CPA Detective, for example, help advertisers and networks identify traffic generation and detect affiliate fraud. But we recognise, to the best of our knowledge, that these have not been tested in a PRS context.

In light of comments received, we propose to change the following items in Paragraph 10.5 of the Guidance:

- Closely monitor their affiliate marketing, particularly in response to consumer complaints ~~unexplained spikes in~~ *and abnormal* traffic *patterns.* ~~to their service~~ ~~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* ~~and tracking tools~~ are in the interest of the PRS industry ~~and requires limited capital outlay~~.
- 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,* ~~utilise effective tracking~~ and monitor~~ing tools~~ 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 .

MobileMinded and Empello argued that affiliate networks mask the identity of their affiliate marketers from their clients, i.e. the Level 2 provider, and therefore a number of our suggestions are, in their opinion, technically impossible. We acknowledge that this is sometimes the case but we would question why a Level 2 provider would wish to start contracting with a totally 'blind' network that offers zero transparency or guarantees; without robust contractual arrangements, a blind network is capable of delivering rogue traffic that is unlikely to convert legitimately.

However, if the network provides sufficient traffic analysis but hides the exact identity of its sources, gaining a good understanding of your traffic and its sources is still very much possible. Networks should provide affiliate IDs, which should be a basis on which to analyse traffic and identify any abnormal activity. While it may be very difficult to always trace specific consumer experiences, affiliate IDs are a good basis to explore non-compliant consumer journeys.

Having consulted with a number of affiliate networks during the process of analysing responses, we are aware of a number that will contract with PRS and offer higher levels of transparency than blind networks. This may come at a higher cost but we do not think this is disproportionate given the need to ensure consumer protection. Indeed, as the IAB adhered to in their response, a number of affiliate networks are committed to good practice. We therefore do not propose to change the Guidance any further on this matter.

Following discussions during and after the consultation period, a number of stakeholders have asked PhonepayPlus to expand on our due diligence and risk assessment and control (DDRAC) expectations. We are happy to do so but would underline that due diligence and

risks assessment are not a 'tick box exercise', but an ongoing process that is designed to help meet the outcomes in the Code. As such, providers should constantly be looking to assess and improve their DDRAC practice. Currently Paragraph 10.4 reads:

> PhonepayPlus expects PRS providers to take account of PhonepayPlus' previous Guidance on Due Diligence and Risk Assessment and Control on Clients. In particular, PRS providers should undertake effective due diligence on any affiliate marketer that they are seeking to engage. As stated in article 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.

Therefore we have decided to add several suggestions to Paragraph 10.4 to help providers meet their ongoing DDRAC responsibilities. Again this is by no means a 'tick-box' list but, in keeping with our outcomes-based approach to regulation, these are designed to assist Level 2 providers in assessing the suitability of any affiliate that they may contract with.

> 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):
>
> - Companies checks;
> - Reputational checks through Google, 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 ongoing;
> - Whether the affiliate network 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, PECR, the CAP Code and relevant consumer protection laws;
> - How the affiliate network sources its traffic. For example, does it source its traffic from file-sharing websites (this will likely result in increased risk);
> - If the affiliate network sub-contracts with other affiliate networks in doing so (which will amplify any risk) and how it sources and vets its individual affiliates;
> - Whether the affiliate network is willing to explain where and in what terms it plans to place your advertising;
> - 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 network in question has fraud detection systems and monitoring tools in place;
> - Whether the affiliate network is prepared to run its service on a trial basis.

While the onus is on Level 2s to conduct risk assessment and control on the affiliate networks with whom they intend to contract, Level 1 providers should also ensure their due

diligence and risk assessment controls are sufficient to meet the outcomes set out in the Code. Currently, Paragraph 10.6 of the Guidance includes the following:

> 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.

In addition to this, we propose to add the following for the sake of clarity:

> We recommend that Level 1 providers conduct a range of checks on their clients, including (but not limited to):
>
> - Check which affiliates or affiliate networks your client contracts with, identifying any affiliate which might pose a significant risk;
> - Ensure your client has appropriate contractual arrangements and risk control processes in place to deal with affiliate marketing and misleading digital marketing more generally;
> - Undertake thorough and frequent checks to ensure your client's promotional material meets the outcomes set out in the Code;
> - Monitor activity for abnormal service behaviour on an ongoing basis;
> - Generally ensure that your client carries out the sort of DDRAC processes set out in Paragraph 10.4.

On the issue of withholds, opinions varied. Empello argued that withholding payments is an important weapon in the Level 2 provider's armoury against rogue affiliates. When first contracting with a network, Buongiorno said that they delay the first few months of payment. On the other hand, Goverifyit argued that withholding payment may not work in practice because networks are generally paid weekly. In preparing this statement, we consulted with affiliate networks that contract with PRS who told us that their general payment terms were 30 days, although a few ask for initial upfront payments. We recommend that providers consider carefully the risks associated with affiliate networks requesting upfront payment. However we do not propose to change the draft Guidance on this issue.

Annex A

(Highlighted text in the following document denotes changes to the Guidance since its draft publication)

General Guidance Note on Digital Marketing and Promotions

Who should read this?

Any provider that promotes its premium rate service (PRS) using forms of digital marketing.

What is the purpose of this Guidance?

To ensure consumers are protected from potential harm and to assist all companies marketing PRS in the digital space to better understand and comply with the Code of Practice (the Code). It sets out PhonepayPlus' expectations related to compliant digital marketing and provides some examples of what might be considered misleading. This Guidance supports previous work, the General Guidance on Promotions and Promotional Material, and builds on the 'Misleading digital marketing of premium rate services' compliance update issued in February 2012. Before reading this Guidance, providers should familiarise themselves with the expectations set out in both of those publications.

What are the key points?

The digital marketing of PRS is increasingly prevalent. Whilst this is a very natural progression and, in most instances, entirely compliant with the Code, PhonepayPlus has noticed, both through Tribunal adjudications and complaint numbers, that certain practices might be found to contravene the Code. Practices of concern are likely to be found to contravene one (or more) of three outcomes in the Code: 'transparency', 'fairness' and 'privacy'.

This Guidance is designed to assist PRS providers in ensuring that their digital marketing meets PhonepayPlus' expectations in relation to compliance with the Code. The main issues for providers to be aware of are:

- Pricing information
- Misleading promotions
- Attracting consumers on false pretences
- The right to privacy

Providers also need to ensure that they have adequate control over marketing that is done on their behalf by third parties, such as affiliate marketers. A Tribunal is highly unlikely to accept arguments that it was the actions of an affiliate that was responsible for a breach of the Code as justification for avoiding liability under the Code for that breach, although such action may be taken into account in terms of mitigation.

What is digital marketing and why might it be a problem?

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 are entirely legitimate, compliant with the Code, generate revenue for the industry, drive innovation, allow consumers to engage with PRS and do not cause undue consumer harm.

1.2 At the time of writing, we have identified eight broad practices that are potentially problematic that can be split into practices which are always misleading and practices which are problematic if they are done in a misleading way. These are as follows:

Practices which are always misleading

- Typosquatting
- Clickjacking
- Likejacking

Practices which are mainstream, but where we have seen some misleading examples in a PRS context

- Banner ads, pop-ups and pop-unders
- Search engine marketing (SEM) and Search Engine Optimisation (SEO)

Practices which are highly likely to mislead consumers in PRS

- Content lockers
- Adware

And

- Unsolicited Electronic Communications (Spam)

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 emerging practices are likely to meet the outcomes set out in the Code. The fact that an unfair practice is not listed in this Guidance is unlikely to be treated by the Tribunal as a defence to an alleged breach of the Code.

1.3 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.

1.4 Our principal concerns relate to three outcomes in the Code: transparency, fairness and privacy.

- Transparency – Rule 2.2.1 of the Code states: "Consumers of premium rate services must be fully and clearly informed of all information likely to influence the decision to purchase, including the cost, before any purchase is made." As such, consumers must be presented with all vital information, including the price, relating to a PRS service before they commit to purchasing it.
- Fairness – Rule 2.3.2 of the Code states: "Premium rate services must not mislead or be likely to mislead in any way." If consumers are to have confidence in the PRS industry, it is important that they are not intentionally misled.
- Privacy – Rule 2.4.1 of the Code states: "Providers must ensure that premium rate services do not cause the unreasonable invasion of consumers' privacy." Consumer consent must be knowing and clearly identifiable.

1.5 The following practices may be found by a Tribunal to be in breach of the abovementioned paragraphs of the Code.

Typosquatting

2.1 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.

2.2 In PRS terms, 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 association with a trusted brand.

2.3 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 to which it does not have an association, in a way that is likely to mislead consumers about the nature of the service being offered, a PhonepayPlus Tribunal is highly likely to consider it in breach of Rule 2.3.2.

Clickjacking

3.1 Often referred to as 'UI readdress attack', clickjacking is designed to hijack clicks from one webpage to another. By clicking on a disguised link (the link may be hidden using transparent i-frames), 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.

3.2 In PRS terms, the consumer will be misled into redirecting to a website offering a PRS promotion, which may lead to a purchase on 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.

3.3 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.

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

3.5 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.

Likejacking

4.1 Likejacking is a form of clickjacking targeting 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, thus propagating it under false pretences. The deception works in the same way as clickjacking using a transparent iframe to disguise a link.

4.2 The link will also 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.

4.3 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.

4.4 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. Records of consent should be made available to PhonepayPlus upon request.

Misleading Banner Ads, Pop-ups and Pop-unders

5.1 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.

5.2 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.

5.3 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.

5.4 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.

Misleading Search Engine Marketing and Search Engine Optimisation

6.1 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 means for PRS providers to market their products. However, providers might use misleading terms in order to artificially boost their search engine ranking. This practice is highly likely to be found misleading by the Tribunal.

6.2 Providers are expected to use adwords 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.

6.3 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.

Content lockers

7.1 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 other misleading digital marketing. These include clickjacking, likejaking and SEM/SEO.

7.2 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.

7.3 Ransomware 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.

7.4 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 ~~highly~~ likely to be considered misleading.~~, especially where the~~ 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.

Adware

8.1 Adware 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.

8.2 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.

Unsolicited Electronic Communications (Spam)

9.1 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.

9.2 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 and Consent to Charge.

9.3 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 ~~there is explicit and auditable consent~~ 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 and Consent to Charge.

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

10.1 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.

10.2 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 marketer breaches 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.

10.3 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.

10.4 PhonepayPlus expects PRS providers to take account of PhonepayPlus' previous Guidance on Due Diligence and Risk Assessment and Control 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):

- Companies checks;
- Reputational checks through Google, 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 ongoing;
- Whether the affiliate network 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, PECR, the CAP Code and relevant consumer protection laws;
- How the affiliate network sources its traffic. For example, does it source its traffic from file-sharing websites (this will likely result in increased risk);
- If the affiliate network sub-contracts with other affiliate networks in doing so (which will amplify any risk) and how it sources and vets individual affiliates
- Whether the affiliate network is willing to explain where and in what terms it plans to place your advertising;
- 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 network in question has fraud detection systems and monitoring tools in place;
- Whether the affiliate network is prepared to run its service on a trial basis.

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

- Place clear expectations on their affiliate networks and 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):
    - Price and other key information should be clearly stated;
    - Any marketing be directly related to the PRS offering i.e. not unrelated and misleading;

    - 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, ~~unexplained spikes in~~ abnormal traffic patterns ~~to their service~~ 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 ~~and tracking tools~~ are in the interest of the PRS industry ~~and requires limited capital outlay~~.
- 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, ~~utilise effective tracking~~ and monitor~~ing tools~~ 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.
- Make it clear to affiliate networks and marketers (and reflect this in the contract) that any failure to comply with the expectations set will result in suspension of payments.
- If an affiliate network or marketer is unable to meet the expectations placed on it, providers are advised to review their relationship with the affiliate marketer or network concerned.
- Keep clear records of any activity, and make them available to PhonepayPlus upon request.

10.6 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):

- Check which affiliates or affiliate networks your client contracts with, identifying any affiliate that might pose a significant risk;
- Ensure your client has appropriate contractual arrangements and risk control processes in place to deal with affiliate marketing and misleading digital marketing more generally;
- Undertake thorough and frequent checks to ensure your client's promotional material meets the outcomes set out in the Code;
- Monitor activity for abnormal service behaviour on an ongoing basis;
- Generally ensure that your client carries out the sort of DDRAC processes set out in Paragraph 10.4.

The role of General Guidance

11.1 General Guidance does not form part of the Code of Practice; neither is it absolutely binding on PhonepayPlus' Code Compliance Panel Tribunal ('the Tribunal'). However, we intend for it to assist all Network operators and providers as to how compliance with the Code can be achieved.

11.2 Network operators or providers are free to disregard Guidance where they feel that the same standard and expectation of consumer protection can be met by some other means. Should consumer harm occur, the Tribunal may examine the provider's alternative actions (including no action), and whether those actions have achieved compliance with the Code. If they have not taken any action to comply with the Code, then such behaviour is likely to be regarded as a serious breach.