Code Compliance Panel

Tribunal Decision

PhonepayPlus

Tribunal Meeting Number 141 / Case 3
Case Reference: 13686
Level 2 provider: David Frier Trading as Marhill Consultants (Gibraltar)
Type of Service: Competition - non-scratchcard
Level 1 provider: Zamano Solutions Ltd (Dublin, Ireland)
Network operator: All Mobile Network operators

THIS CASE WAS BROUGHT AGAINST THE LEVEL 2 PROVIDER UNDER PARAGRAPH 4.4 OF THE CODE

BACKGROUND

Between 11 March 2013 and 9 October 2013, PhonepayPlus received 241 complaints from consumers in relation to a competition subscription service (the "**Service**") operated by the Level 2 provider David Frier trading as Marhill Consultants, under the brand name "Play4Prizes". The Service operated on the premium rate shortcode 88990 and cost £4.50 per week. The Level 1 provider was Zamano Solutions Ltd. The Service operated between September 2012 and 13 June 2013 when it was voluntarily suspended by the Level 1 provider. The Service was promoted online using affiliate marketing.

Consumers subscribed to the Service (using a key word SMS or an online PIN code opt-in) and were entered into a weekly draw to win prizes such as iPhones, iPads or £50.

Complainants either stated that they had received unsolicited, reverse-billed text messages and that they had not engaged with the Service, or acknowledged engaging with the Service but stated that they believed it was free. PhonepayPlus monitoring revealed concerns about affiliate marketing promotions for the Service.

The Investigation

The Executive conducted this matter as a Track 2 investigation in accordance with paragraph 4.4 of the PhonepayPlus Code of Practice (12th Edition) (the "**Code**").

The Executive sent a breach letter to the Level 2 provider on 3 December 2013. Within the breach letter the Executive raised the following breaches of the Code:

- Rule 2.3.1 - Fair and equitable treatment
- Rule 2.3.2 – Misleading

The Level 2 provider responded on 17 December 2013. On 9 January 2014, after hearing informal representations made on the Level 2 provider's behalf by the Level 1 provider, the Tribunal reached a decision on the breaches raised by the Executive.

SUBMISSIONS AND CONCLUSIONS

Monitoring

On 1 March 2013, the PhonepayPlus Research and Market Intelligence (the "**RMIT**") monitored the Service after being redirected from the Mobile Data Association website to an affiliate marketing promotion for the Service.

The RMIT searched the Google search engine for the Mobile Data Association website and clicked on the first search result which was a link to the official Mobile Data Association website (**Appendix A**). Upon clicking on the link, the RMIT was immediately redirected to an affiliate marketing promotion for the Service (**Appendix B**). The RMIT used an online analysis tool to scan the Mobile Data Association's website for malicious activity (**Appendix C**). The result revealed that the legitimate website had been hacked and visitors from the Google search engine had been redirected to the URL "http://tinyurl.com/aupaxfh". The RMIT used a traffic recording programme called "Fiddler" to show the URL journey after selecting the link to the Mobile Data Association website. This also revealed that the RMIT had been unknowingly diverted.

The promotion invited the RMIT to answer "Yes or "No" to be "today's iPhone 4S winner". The RMIT selected "Yes" on the affiliate marketing promotion (**Appendix B**) and was directed to a webpage which stated:

"Great News!
You have been selected for a chance to win an Apple iPhone5!
Click "Ok" for details."

After selecting "OK" the RMIT maximised the browser underneath the page and selected a prize (**Appendix D**). The RMIT was directed to a Service landing page (**Appendix E**). The Executive noted that the first time a consumer would have been made aware that the promotion was for a premium rate service was by reading the terms and conditions shown on the Service landing page.

Complaints

The Executive noted the content of all the complaints received, examples of which include:

"Consumer was on BT page and a pop up window came up saying he can win a [sic] iphone or a ipad he thought it was a competition service for BT he thought he was doing some survey. Consumer saying he saw no pricing information."

"Survey on a sight he visits regularly. He was locked into it and under the impression it was to do with the dating site."

"The 'service' was presented as a chance to win a prize following completion of a survey on the web which was presented as a survey from the Met office. This was in a pop up screen that came up when looking at the Met office web site over a motorway service WLAN. However teh Met office confirmed that they had no involvement in this and hence it was a scam to charge for a primiam rate service. [sic]"

ALLEGED BREACH 1
Rule 2.3.1
"Consumers of premium rate services must be treated fairly and equitably."

1. The Executive submitted that the Level 2 provider was responsible for a breach of rule 2.3.1 of the Code as consumers were not treated fairly and equitably as a result of malware, which automatically diverted consumers to affiliate marketing promotions for the Service without their knowledge.

   The Executive relied on the monitoring of the Service conducted by the RMIT and detailed above in the "Background" section. In addition, the Executive relied on data taken from

www.alexa.com (a website information company which provides free website analytics). The data revealed websites that consumers had visited immediately before arriving on the Service landing page. The RMIT was directed to the Service landing page from the visitorgift.com website. According to the Alexa data 5.07% of the traffic to the Service landing page was from visitorgift.com. Consequently, the Executive submitted that a significant percentage of the Service's traffic came from the visitorgift.com website and a significant number of consumers were likely to have experienced a similar consumer journey to that experienced in the monitoring.

The Executive asserted that consumers were not treated fairly as they were maliciously diverted to a promotion for the Service after they had selected the correct link for the official Mobile Data Association website (and/or any other hacked website). Accordingly, the Executive submitted that rule 2.3.1 of the Code had been breached.

2. The Level 2 provider denied that a breach of the Code had occurred and stated that it had not treated consumers unfairly, as it did not allow the affiliate marketers for its Service to promote the Service in a way where consumers were forced to visit the Service landing page. It stated that the hacking of the Mobile Data Association website occurred without its knowledge and consent. In addition, it did not believe that the affiliate marketers in question would have been aware of where the traffic was coming from as it explained that they brought traffic on a blind network. The Level 2 provider asserted that it was incorrect and unfair to imply that it had any involvement in this malpractice.

The Level 2 provider accepted that the Executive's monitoring showed that it was diverted from the URL that it had selected, but it strongly maintained that consumers were not treated unfairly on the affiliate promotional pre-landing page or on the Service promotional webpages. Further, it asserted that the pricing was clearly displayed beside the main call to action on the MSISDN entry and PIN entry webpages (**Appendix F**).

The Level 2 provider stated that the affiliate marketer behind the visitorgift.com was not the recipient of all the traffic from the Mobile Data Association website as the affiliate network would have been buying traffic from an advertising network along with many other affiliate networks.

The Level 2 provider stated that "any perceived unfair treatment of consumers is negligible" due to the following reasons:

i) It noted that the Alexa data was unable to confirm where consumers visited immediately following the Mobile Data Association website due to a lack of data. The website was ranked globally as the 2,416,169 most popular website. There was no significant data available on Alexa, regarding the sites consumers visited prior to attempting to visit the Mobile Data Association website.

ii) Re-direct traffic is a very cheap source of traffic as it is untargeted and produces a low conversion rate.

iii) The diversion only occurred on certain search engines and had the RMIT used Google Chrome (which is the most popular search engine with an estimated 53% of the market) the diversion would have been blocked, which it demonstrated with a screenshot of the Google Chrome webpage.

iv) The Mobile Data Association website was likely to have been exploited for a short period of time. The likelihood of any major websites being hacked was extremely unlikely.

The Level 2 provider summarised a number of controls the Level 1 provider had put in place, on the Level 2 provider's behalf, to manage the risks that were associated with affiliate marketing which include:

i) Pre-approval of the affiliate marketing "lead in" webpages.
ii) Marketing partner was required to provide the full URL referrer for all "clicks" to the Service. Referrers are checked on a daily basis to ensure that they meet its compliance standards.
iii) "Wild monitoring", which involves searching the web looking for the Service's promotions to identify concerns.
iv) Blacklisting publishers who have breached the prohibited practices (evidenced by correspondence addressing previous issues that had been identified by the Level 2 provider).
v) Notification of the Level 2 provider's prohibited practices to the affiliate networks.
vi) Affiliate marketers are required to agree to stringent terms and conditions containing prohibitions.

The Level 2 provider stated that on this occasion the controls in place did not capture the non-compliant promotions as:

i) The volume of traffic generated from the visitorgift.com website would have been relatively small (it did not know the exact figure) and consequently it would have been difficult to detect in day-to-day monitoring.
ii) The webpage submitted for approval did not contain the names of any trusted brand names. Survey style landing pages had previously been submitted to PhonepayPlus and they were not deemed to be non-compliant. The use of survey style pages have been added to its list of non-permissible marketing practices from July 2013.
iii) When the marketing partner gave the Level 2 provider the URL referrer it had hidden an element of the URL that detailed names of any sites or brands that would have been seen by the consumer. The Level 2 provider reviewed the referrers but only saw "Visitor Survey" in the header and not that of a trusted brand name.
iv) The Level 2 provider submitted that search term re-direction was not commonly known about by premium rate service providers. It stated that there had not been any industry notification or PhonepayPlus adjudications relating to the use of Adware. The Level 2 provider's monitoring focused on movie downloads and streaming sites.

The Level 2 stated that the time stamps on the RMIT monitoring did not follow in sequence, which it stated meant that the RMIT did not follow the consumer journey described. The Level 2 provider invited the Tribunal to disregard this evidence.

During informal representations, the Level 1 provider made representations on behalf of the Level 2 provider. The Level 1 provider stated that the Service was a white label product provided by the Level 1 provider. It included the billing platform and provided assistance with the content management, subscriptions, prize fulfilment, customer service and marketing best practice. However it confirmed that the Level 2 provider was responsible for the marketing of the Service, although the Level 1 provider had controls in place to assist with monitoring promotions of the Service.

The Level 1 provider expanded upon the Level 2 provider's written submissions and stated that it had no reason to doubt that the Mobile Data Association website had been hacked. By way of background, the Level 1 provider explained the nature of the Service and the flow

on the Service's promotional webpages. The Level 1 provider asserted that a consumer would have been fully aware of the nature and the pricing of the Service.

In relation to the Executive's evidence from Alexa, the Level 1 provider stated that the analytics showed the traffic to the Service's website but it was not able to show the number of consumers who subscribed to the Service. The Level 2 provider stated that the Alexa data is collated from users who have the Alexa toolbar installed and therefore the figures are only indicative.

The Level 1 provider stated that it had conducted monitoring of the Service in Ireland by using a proxy that mimicked a UK IP address. It accepted that this was not as good as monitoring in the UK as malware may have been able to detect that it had used a proxy.

The Level 1 provider drew the Tribunal's attention to the length of time it had taken the Executive to investigate the breaches and stated that it had not been able to operate and/or promote the Service which had had a considerable effect on its revenue.

3. The Tribunal considered the evidence and submissions before it, including the Level 1 and Level 2 provider's detailed written and oral submissions. The Tribunal found that, in light of the monitoring evidence, consumers had been inadvertently diverted to a website, without their knowledge, which had no connection to the initial search. As a result, consumers were inadvertently led to a premium rate service and therefore had not been treated fairly and equitably. Further, the Tribunal noted the significant number of consistent complainant accounts concerning other websites where consumers had inadvertently been led to the Service landing page. Consequently, and for the reasons given by the Executive, the Tribunal found that consumers had not been treated fairly and equitably. Accordingly, the Tribunal upheld a breach of rule 2.3.1 of the Code.

Decision: UPHELD

ALLEGED BREACH 2
Rule 2.3.2
"Premium rate services must not mislead or be likely to mislead in any way."

1. The Executive submitted that the Level 2 provider had breached rule 2.3.2 of the Code as consumers were misled into using the Service for the following reasons:

   i) Consumers were misled into believing that they were completing a survey/entering a competition for a trusted brand (or that the survey/competition was affiliated to a trusted brand).
   ii) Consumers were misled into believing that if they answered the questions they would have a chance of winning a prize, when in fact they were required to enter a premium rate subscription service at a cost of £4.50 per week to have the opportunity to win a prize.
   iii) Wording contained within the promotions created a false sense of urgency that was designed to encourage consumers to interact with the Service.

Guidance

The Executive relied on the content of the PhonepayPlus Guidance on "Promotions and promotional material". The Guidance states:

Misleading promotions

Paragraph 3.1

"If consumers are to have trust and confidence in using PRS, it is important that they have available all the key information about a service as part of their consideration of whether to make a purchase or not. For this reason, it is important that promotions do not mislead consumers by stating an untruth or half-truth. It is also important that promotions do not omit, or make insufficiently prominent, an important term or condition likely to affect their decision to use the service."

Controlling risk when using affiliate marketers

Paragraph 6.2

"In these circumstances, PhonepayPlus recognises that the Level 2 provider, while retaining responsibility for the promotion under the PhonepayPlus Code of Practice, may not have immediate, day-to-day control of each individual action that an affiliate takes. However, the use of affiliates to market PRS products on a provider's behalf does carry a greater risk than marketing which is under the direct, day-to-day control of the provider."

The Executive relied on the monitoring of the Service conducted on 1 March 2013 by the RMIT and the complainants accounts detailed in the Background section.

Reason one: Consumers were misled into believing that they were completing a survey/entering a competition for a trusted brand (or that the survey/competition was affiliated to a trusted brand)

The Executive noted the content of the affiliate marketing promotions that the RMIT was directed to during its monitoring session (**Appendix D**). The Executive asserted that consumers were likely to believe that the survey was connected to the website that they had attempted to access. In addition, the Level 2 provider had provided the Executive with an example of an approved affiliate marketing campaign which was entitled "Visitor Survey". The Executive asserted that, although both screenshots did not contain the brand name, given that a consumer was redirected and/or they had viewed a webpage entitled "Visitor Survey" consumers were likely to be misled into believing that the survey/ competition was affiliated with a trusted brand.

Reason two: Consumers were misled into believing that if they answered the questions they would have a chance of winning a prize, when in fact they were required to enter a premium rate subscription service at a cost of £4.50 per week to have the opportunity to win a prize.

The Executive asserted that the affiliate marketing promotion (**Appendix D**) was likely to have misled consumers into believing that once they had correctly answered the question they would then be entered into the prize draw. The webpage contained no indication that a consumer would need to subscribe to the Service to have an opportunity to win a prize.

Further, the affiliate marketing promotion provided by the Level 2 provider entitled "Visitor Survey" created the impression that by completing the survey consumers would have a chance to win a prize. The webpage stated:

"You've been selected to take part in this anonymous survey. Please take our 30 second marketing questionnaire and to say "thank you" you will have the opportunity to win the new Apple ® iPhone 5 or iPad".

Following this, consumers were invited to select a prize but there was no indication that a consumer would need to subscribe to the Service to have an opportunity to win a prize.

Reason three: Wording contained within the promotions created a false sense of urgency that was designed to encourage the consumer to interact with the Service.

The Executive asserted that the following wording contained within the promotions created a false sense of urgency:

i) "Click the "Yes" button below to try and win before time runs out."
ii) "Please respond NOW before other visitors have a chance to win the prize"
iii) "You have been selected for a chance to win an Apple ® iPhone5!

The Executive submitted that the wording was misleading as the terms and conditions stated that the competition closing date was 3 March 2013, two days after the RMIT's monitoring session. In addition, the Executive submitted that some of the wording was likely to mislead consumers into believing that they had been specifically selected to participate when all consumers who were directed to the affiliate marketing promotional webpage would view the same message.

Consequently, the Executive submitted that in light of the features of the affiliate marketing promotion, the Service misled was likely to have misled consumers into believing that they were completing a survey/competition for a trusted brand, that completion of the survey/questions would automatically enter them into a prize draw and that there was a sense of urgency to interact with the Service. Accordingly, the Executive submitted that for the reasons outlined above rule 2.3.2 of the Code had been breached.

2. The Level 2 provider denied that consumers had been misled into interacting with the Service for the three reasons outlined by the Executive. The Level 2 provider explained that it was unaware that it was potentially in receipt of re-direct traffic from hacked websites. In any event, the Level 2 provider asserted that the volume of re-direct traffic from potentially hacked sites was "miniscule".

Specifically in relation to reason one outlined by the Executive above, the Level 2 provider stated that at no point in the promotional process were customers informed that they were completing a survey or answering a question for a trusted brand and it disputed that any evidence of this had been presented by the Executive. The Level 2 provider stated that a consumer who selected the Mobile Data Association website and was diverted to the affiliate marketing promotion for the Service would not necessarily have believed that the two webpages were connected, as the Mobile Data Association brand was not used at any point during the promotional process.

In relation to the screenshot entitled "Visitor Survey" provided to the Executive by the Level 2 provider, it disputed that the title was likely to mislead consumers as it was not associated with a trusted brand and in any event there was no evidence that the page was associated with re-directed traffic. Further, the Level 2 provider stated that the Executive had previously had this brought to its attention on 30 November 2013 and in relation to a similar case in February 2012, yet it did not raise concerns.

The Level 2 provider stated that the screenshots produced by the Executive did not show the complete consumer journey as the time stamps did not follow in sequence. In addition, the data from Alexa demonstrated that there was an insufficient volume of traffic on the Mobile Data Association website for it to provide full statistics and therefore the number of affected consumers was "miniscule".

In relation to reason two advanced by the Executive, the Level 2 provider stated that consumers were not misled into believing that if they completed a survey/answered questions they would have a chance of winning a prize without entering a premium rate service. It stated that consumers were advised in the terms and conditions that there was free route of entry to the Service. In addition, throughout the entire consumer journey consumers were informed that they have a chance to win and they are not told that it was a certainty. The language used was always conditional, "you will have an opportunity to win a prize", "you have a chance to win" and "you could win (1) prize from the list below". The Level 2 provider asserted that the conditional language was continued on the Service landing page.

In relation to reason three advanced by the Executive, the Level 2 provider stated the terminology used in the promotional material was not likely to mislead consumers. The format had been used for a number of years and had been submitted to PhonepayPlus on a number of occasions by both the Level 2 and Level 1 provider. Specifically, in relation to the wording, "before time runs out", the Level 2 provider stated that this was reasonable because there was a closing date for the competition. Wording such as "Respond now" is a universally accepted marketing phrase similar to, "Hurry while stocks last". In conclusion, it stated that it did not believe that it created a misleading false sense of urgency.

The Level 2 provider stated that it accepted:

> "...that randomness only occurs in the process when winners are selected by Promo Veritas. With that in mind, we suggest that wording such as Friday afternoon visitors to our site have a chance to be our luck winner. You are a potential winner!".

The Level 2 provider stated that since April 2013 the complaint levels to the Service had dramatically decreased and this had been recognised by PhonepayPlus in a presentation at an AIME Regulatory Roundtable meeting on 27 November 2013. The Level 2 provider stated that this was as a result of increased affiliate marketing monitoring and the application of stricter marketing rules and regulations.

During informal representations, the Level 1 provider made representations on behalf of the Level 2 provider. In relation to the second reason outlined by the Executive, the Level 1 provider strongly refuted that a breach had occurred as it stated that it was always made clear to consumers that they only had a "chance" to win a prize. The Level 1 provider stated it was a cumulative process and by the time the consumer reached the Service webpages consumers had been informed of all the key Service information and it was made clear that it was a premium rate service. The terms and conditions and pricing information were on the Service webpages close to the call to action.

The Level 1 provider stated that it was "bad practice" for traffic to come from a hacked website.

The Level 2 provider reiterated the measures and controls it had in place to manage the risks posed by affiliate marketing as detailed above in its submissions for the breach of rule 2.3.1. It also stated that it has always used online chat forms/ blogs to identify problems with the Service but since June 2013, it has started to document and record its findings.

In respect of the wording used on the promotions, the Level 1 provider stated it believed that providing it had not told the consumer that it had won a price, when it only had a "chance", it would be compliant.

The Level 1 provider stated that the Level 2 provider had not been able to ascertain how many consumers had come to the Service via the hacked website as it had not had sight of the sub-publisher's identification code. Therefore, it conceded that it was an assumption that the traffic was miniscule.

3. The Tribunal considered the evidence and submissions before it. The Tribunal noted the affiliate marketing promotion provided by the Level 2 provider entitled "Visitor Survey" and the number of consistent complainant accounts stating that consumers believed the survey was connected to the website they had intended to visit. The Tribunal found that consumers were likely to have been misled into completing the survey and/or answering questions, as the promotions created the mistaken impression that the survey was connected to a trusted brand. The Tribunal did not accept the Level 2 provider's assertion that the amount of consumers affected was "miniscule". The Tribunal noted the language used on the affiliate marketing promotions and found that phrases such as, "Great News!" and "You have been selected...", were misleading and likely to create the impression that a consumer was only required to complete the survey to be eligible to win a prize. The Tribunal also found that the language used in the affiliate marketing promotions created a false sense of urgency. The Tribunal noted that the Level 1 provider had stated that its own landing pages were clear and remedied the misleading affiliate marketing promotion. However, the Tribunal did not accept this and found that the overall effect of the consumer journey was misleading. The Tribunal noted that there had recently been a PhonepayPlus Track 1 procedure in relation to the display of pricing information on Service webpages. Consequently, the Tribunal concluded that, for the three reasons outlined by the Executive consumers had been misled. Further, the Tribunal noted that the Level 2 provider was responsible for the content of the promotions. Accordingly, the Tribunal upheld a breach of rule 2.3.2 of the Code.

Decision: UPHELD

SANCTIONS

Initial overall assessment

The Tribunal's initial assessment of the breaches of the Code was as follows:

Rule 2.3.2 - Misleading

The initial assessment of rule 2.3.2 of the Code was **serious**. In determining the initial assessment for this breach of the Code the Tribunal applied the following criterion:

- Serious cases have a clear detrimental impact, directly or indirectly, on consumers and the breach had a clear and damaging impact or potential impact on consumers.

Rule 2.3.1 - Fairness

The initial assessment of rule 2.3.1 of the Code was **serious.** In determining the initial assessment for this breach of the Code the Tribunal applied the following criterion:

- Serious cases have a clear detrimental impact, directly or indirectly, on consumers and the breach had a clear and damaging impact or potential impact on consumers.

The Tribunal's initial assessment was that, overall, the breaches were **serious.**

Final overall assessment

In determining the final overall assessment for the case, the Tribunal took into account the following aggravating factor:

- At the time of the monitoring, there had been a number (approximately 11) of prior adjudications concerning affiliate marketing.

In determining the final overall assessment for the case, the Tribunal did not find any mitigating factors. However, the Tribunal noted that the Level 1 provider on behalf of the Level 2 provider had the following measures in place to identify and mitigate against the risks associated with affiliate marketing:

- Pre-approval of the affiliate marketing "lead in" webpages.
- Marketing partners are required to provide the full URL referrer for all "clicks" to the Service. Referrers are checked on a daily basis to ensure that they meet compliance standards.
- "Wild monitoring", which involves searching the web looking for the Service promotions to identify concerns.
- Blacklisting publishers who have breached the prohibited practices (evidenced by correspondence addressing previous issues that had been identified by the Level 2 provider).
- Notification of the Level 2 provider's prohibited practices to the affiliate networks.
- Affiliate marketers are required to agree to stringent terms and conditions containing prohibitions.

The Tribunal also noted that on being notified of the malware affiliate marketing, the Level 1 provider had taken the following action on the Level 2 provider's behalf:

- Voluntarily suspended the Service.
- Blacklisted the relevant publisher.
- Outsourced UK monitoring to an independent third party Goverifyit.
- Increased its monitoring which was conducted by a dedicated team within the Level 1 provider.
- Imposed traffic restrictions that only permit affiliate marketers to use display and pop-under promotions.
- Efforts made to encourage knowledge sharing amongst Level 1 and 2 providers including assisting in the implementation of an AIME/ GVI "Data room" which acts an early warning sign to providers about non-compliant marketing practices.
- Efforts to encourage Level 2 providers to work directly with affiliate publishers directly rather than the affiliate networks in order to exercise greater control of the promotions for its service.

The Tribunal noted that the Level 2 provider stated it had a "no quibble" refund policy but that it had not provided evidence to demonstrate that refunds had been administered to the complainants.

The Tribunal noted that the PhonepayPlus investigation had taken a considerable period of time and that the Service had not been operational for approximately seven months. Accordingly, the Tribunal noted the potential extent of the Level 2 provider's lost revenue during that period.

The Level 2 provider's revenue in relation to the Service was in the range of Band 1 (£500,000+). Having taken into account the aggravating factor, the Tribunal concluded that the seriousness of the case should be regarded overall as **serious**.

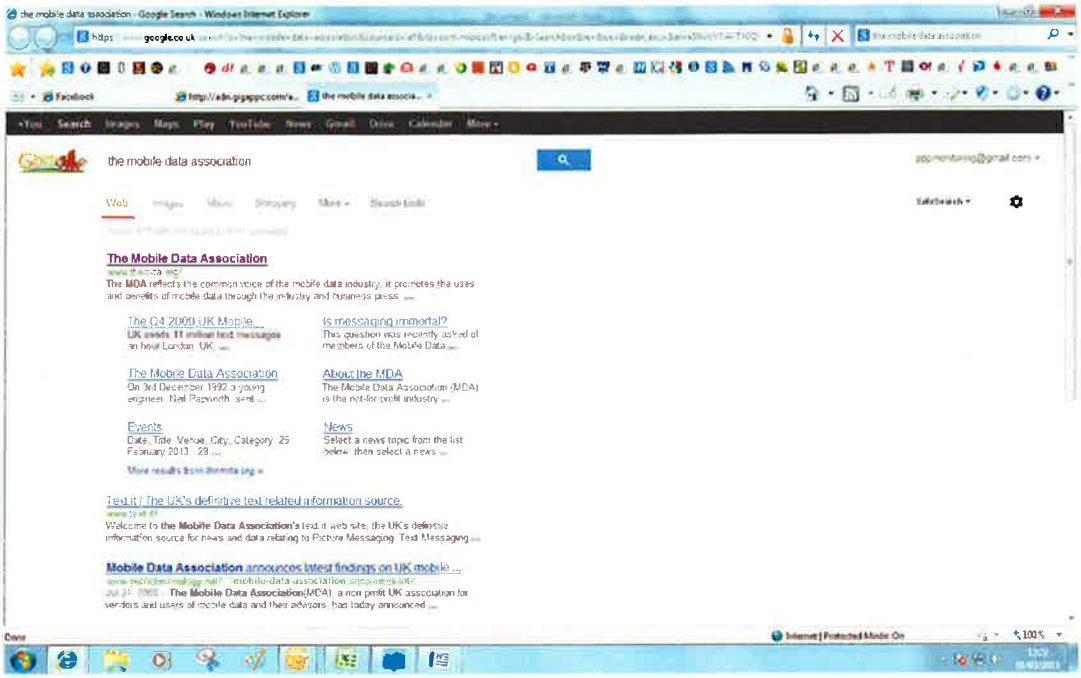
Sanctions Imposed

Having regard to all the circumstances of the case, the Tribunal decided to impose the following sanctions:

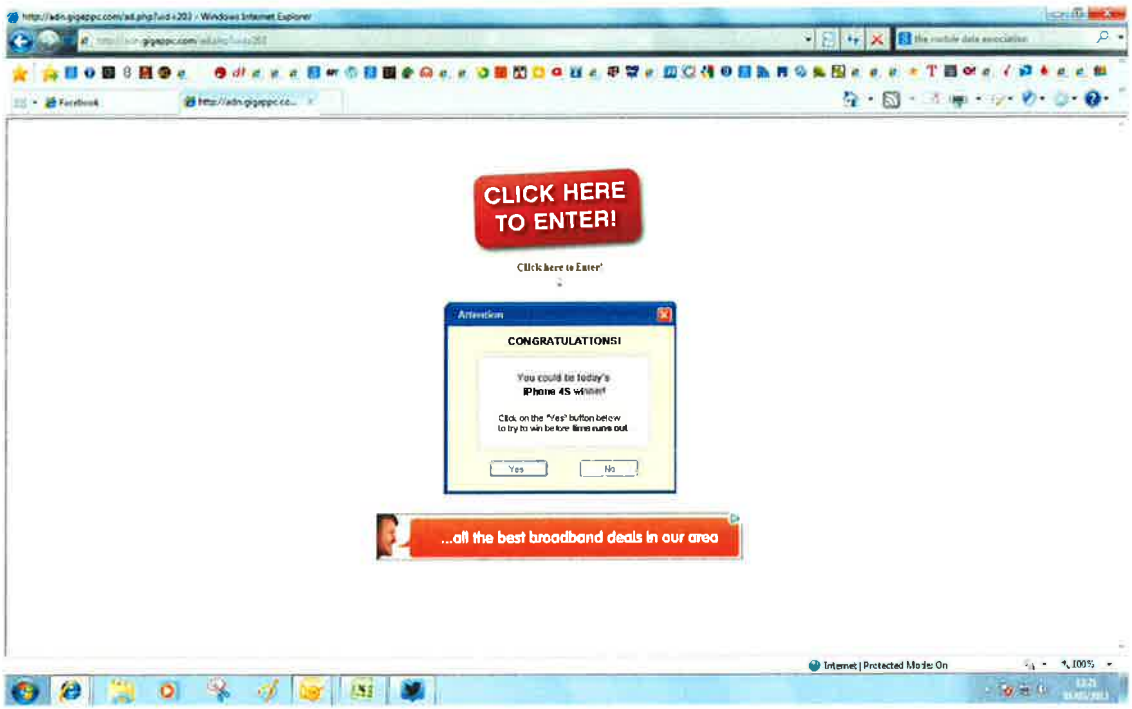
- a formal reprimand;
- a fine of £30,000; and
- a requirement that the Level 2 provider must refund all consumers who claim a refund, for the full amount spent by them on the Service, within 28 days of their claim, save where there is good cause to believe that such claims are not valid, and provide evidence to PhonepayPlus that such refunds have been made.

Appendices

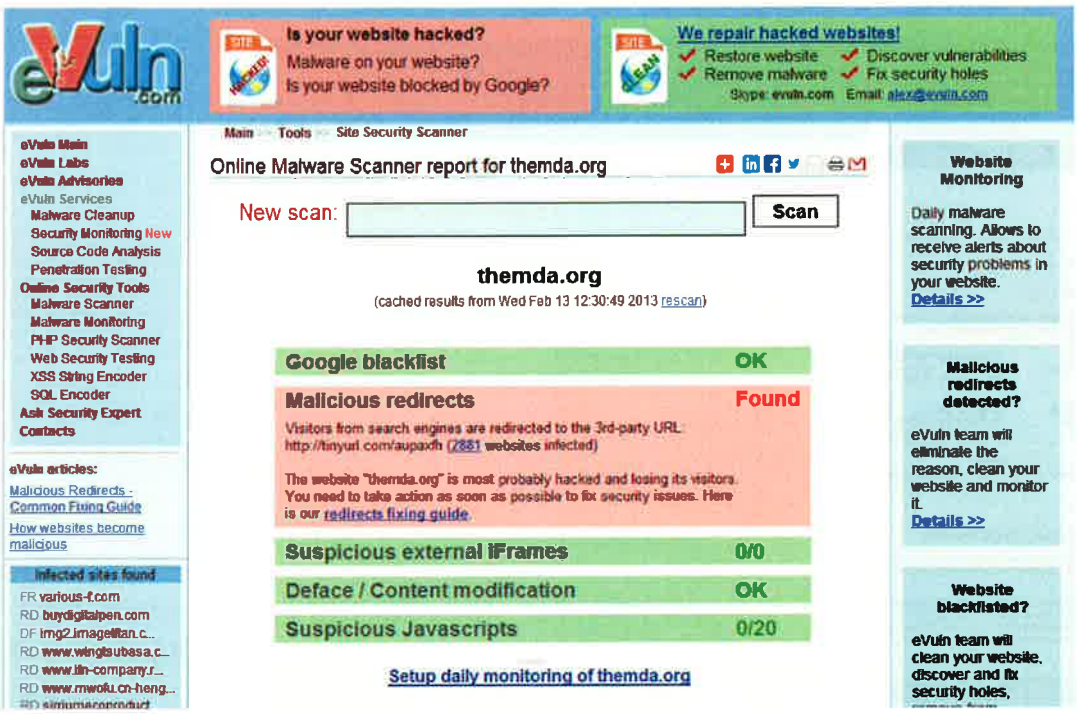
Appendix A: A screenshot of the Google search results showing a link to the official Mobile Data Association website.



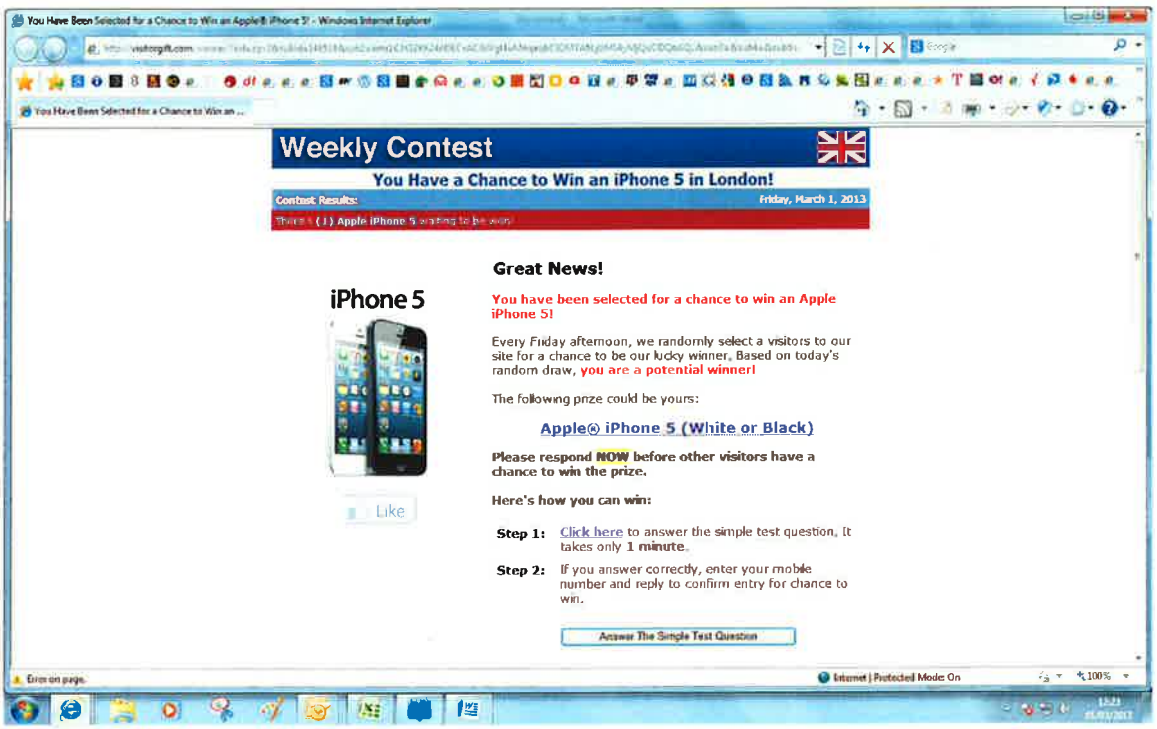
Appendix B: A screenshot of an affiliate marketing promotional webpage for the Service.



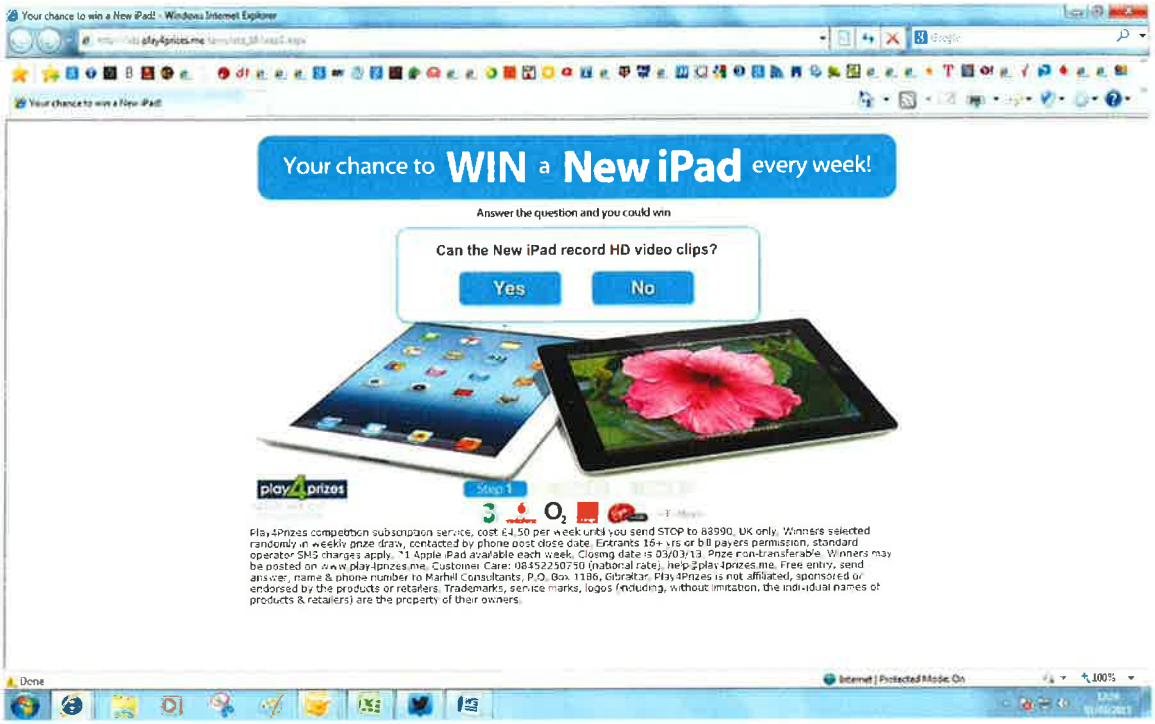
Appendix C: A screenshot of the online malware scanner of the Mobile Data Association website.



Appendix D: A screenshot of the affiliate marketing promotional webpage for the Service.



Appendix E: A screenshot of a Service landing page.



Appendix F: A screenshot provided by the Level 2 provider of the Service means of access webpage: