Tribunal Sitting Number 131 / Case 3

Case Reference: 28902

Level 2 provider	Global Billing Solutions
Type of Service	Competition - non-scratchcard
Level 1 provider	mBlox Limited
Network operator	All Mobile Network operators

THIS CASE WAS BROUGHT AGAINST THE LEVEL 2 PROVIDER UNDER PARAGRAPH 4.5 OF THE CODE

BACKGROUND

The Level 2 provider, Global Billing Solutions operated an online subscription mobile content and competition quiz service using the brand name "Ringaling" (the "**Service**").The Service operated on the premium rate shortcode 80160 at a cost of £4.50 per week and was promoted via affiliate marketeing. The Level 1 provider for the Service was mBlox Limited.

The Service offered consumers the opportunity to access the Services' mobile website and view daily feeds on celebrity gossip, jokes, horoscopes and amusing videos. Consumers were also offered the opportunity to participate in a competition to win a prize, such as Apple products. The competition period was from 1 July 2012 to 31 October 2013.

The Service operated from September 2012 to 9 July 2013.

Serious concerns regarding the promotion of the Service were uncovered as a result of in-house monitoring of the Service conducted by the PhonepayPlus Research and Market Intelligence Team (the "**RMIT**"). The monitoring revealed that affiliate marketing, which generated consumer traffic to the Service, appeared to utilise a form of malware (ransomware) that stopped consumers' internet browsers working, resulting in users being unable to access a large number of popular websites, including Facebook, Ebay, Google. Users were told that they were required to sign up to the Service (and/or other premium rate services) in order to unblock their browsers.

Monitoring

On 28 June 2013, the RMIT visited the website "wifihackpassword.com" (**Appendix A**), which offered users software that purported to enable them to hack into locked Wi-Fi networks. The RMIT clicked on a button marked "Download Now!" which resulted in the software being downloaded. The RMIT opened the file. Instantly a dialogue box appeared and offered a seemingly essential update which the RMIT declined. A further dialogue box appeared that stated:

"Error! Too old version! Update please!". The only option was to click "OK".

The RMIT noted from previous monitoring experiences that accepting the upgrade led to a premium rate service and upon opting-in to the subscription a password, which had no function and which did not allow an upgrade to take place, was provided. The RMIT's internet browser was blocked by the malware and was not unblocked following entry into the service.

The RMIT conducted an additional monitoring session on 2 July 2013. The RMIT opened the

Internet Explorer browser and found it could not access the Google homepage as it was still blocked from the previous monitoring session (**Appendix B**). The browser displayed a webpage that contained a warning that stated:

> "This website has been blocked for you! Steps to access this website again. 1. Click the unlock button below. 2. Pick survey to verify that you are human. 3. Complete Survey. 4. Continue using this website.
>
> "This website has been blocked because of your recent activity. Your actions have been marked as a spam bot like. To visit this website again follow the instructions on the left [see numbered point above]. This is made for security reasons.
>
> "Information about you:
> Country name: UK
> City:
> IP: [IP address redacted]
>
> "Click here to unblock."

In exactly the same manner as in the previous monitoring sessions, the RMIT clicked on the "Click here to unlock" button, a further pop-up appeared which stated (**Appendix C**):

> "WARNING! The content you are browsing is blocked! You must complete at least one offer to have access to this page."

The RMIT selected an option that stated, "Chance to win the All New iPhone 5". The RMIT was directed to one of the Level 2 provider's promotional landing pages which opened in a new browser window.

The RMIT followed the instructions contained on the landing page and answered one multiple choice question. The RMIT were directed to enter its MSISDN and click "Submit" (**Appendix D)**. The next screen prompted the RMIT to send the keyword "WEB" to the shortcode 80160 to opt in to the Service (**Appendix E**). The RMIT monitoring phone received a free text message, again prompting the RMIT to send the trigger keyword to the premium rate shortcode. Upon doing this, the RMIT received subscription confirmation text messages that confirmed the RMIT had successfully opted into the Service and this was also confirmed on the monitoring computer screen.

A notification tab at the bottom of the page indicated a file download was complete but upon clicking on it, the RMIT found the file was password protected and there was no information on where the password could be found. The RMIT noted that the download appeared to have no purpose or function.

The RMIT eventually closed all the browser windows that had been opened during the monitoring session and opened a new Internet Explorer window. The browser displayed the same webpage notifying the browser was blocked (**Appendix B**).

The RMIT selected the "unblock" button and was led back to the "WARNING!" pop-up page that directed the user to complete an "offer" to unblock the browser (**Appendix C**). The RMIT selected the "offer" titled "Your Chance to Win the New iPad Mini" and was directed to one of the Level 2 provider's landing pages. The RMIT completed one multiple choice question and was then prompted to enter its MSISDN and click "Submit" (**Appendix F)**. The RMIT followed the instructed

but a pop-up advised "You are already subscribed". The RMIT finished the monitoring session.

The RMIT noted that completing the "offer" resulted in it subscribing to a premium rate service but its internet browser, which had been blocked by the malware, was not unblocked following entry into the subscription Service.

It is of note that in order to unblock its internet browser the RMIT had to re-boot its desktop in "safe mode" and eliminate all viruses using its existing security software. The Executive noted that it was likely that end users without specialist IT knowledge (and unable to search for a solution on their own computer) would require specialist assistance (potentially at a cost).

The Investigation

The Executive conducted this matter as an Emergency procedure investigation in accordance with paragraph 4.5 of the PhonepayPlus Code of Practice (12th Edition) (the "**Code**").

On 5 July 2013, the Executive notified the findings of its preliminary investigation to a member of the Code Compliance Panel and obtained authorisation to invoke the Emergency procedure in relation to the Service pursuant to paragraph 4.5.2 of the Code. The outcome and a direction to suspend the Service was communicated to both the Level 1 and Level 2 provider on 8 July 2013. On 8 July 2013, the Level 1 provider confirmed that the Service had been suspended and on 10 July 2013, the Level 2 provider confirmed the same.

On 9 July 2013, in accordance with paragraph 4.5.1(c)(iv) of the Code, PhonepayPlus published on its website a notification stating that the Emergency procedure had been invoked.

The Executive sent a breach letter to the Level 2 provider on 23 July 2013. Within the breach letter the Executive raised the following breaches of the Code:

- 2.3.1 - Fair and equitable treatment
- 2.3.2 - Misleading
- 2.5.5 - Avoidance of harm (fear, anxiety, distress and/or offence)
- 2.2.2 - Written information material to the decision to purchase

The Level 2 provider responded on 31 July 2013. On 8 August 2013, and after hearing informal representations made on behalf of the Level 2 provider, the Tribunal reached a decision on the breaches raised by the Executive.

SUBMISSIONS AND CONCLUSIONS

Preliminary issues
Responsibility for affiliate marketing

The Tribunal noted that Level 2 providers are responsible for the Services that they operate; this includes how the services are promoted.

Part 2 of the Code states:
"References to a premium rate service…include all aspects of a service including content, promotion and marketing…Level 2 providers have responsibility for achieving these outcomes by complying with the rules in respect of the provision of the relevant premium rate service."

Paragraph 5.3.8(b) states:
"A Level 2 provider is the person who controls or is responsible for the operation, content and promotion of the relevant premium rate service and/or the use of a facility within the premium rate service."

Further, Code paragraph 5.3.29 states:
"'Promotion' means anything where the intent or effect is, either directly or indirectly, to encourage the use of premium rate services, and the term 'promotional material' shall be construed accordingly."

As a result, the Tribunal found that the Level 2 provider was responsible for the ransomware affiliate marketing promotions which led to the Service landing pages.

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 acted in breach of rule 2.3.1 of the Code as users were not treated fairly and equitably as a result of the malware that blocked users' internet browser functionality.

   The Executive stated that the provision of a premium rate service includes the marketing and promotion of the service. As a result of the above it is clear that a Level 2 provider is responsible for any non-compliance with the Code in relation to the marketing and promotion of its services.

   Monitoring

   The Executive relied on the monitoring of the Service carried out by the RMIT detailed in the "Background" section. The Executive noted that the Service was promoted using affiliate marketing that resulted in users downloading ransomware (a type of malware). The ransomware blocked users' internet browser functionality. Users then entered the Service incurring premium rate charges in order to unblock their browsers.

   The Executive asserted that the malware that blocked users' internet browser functionality interfered with their computers and had the potential to cause inconvenience and unnecessary costs. The Executive asserted that as a result of the ransomware, users were not treated fairly and equitably.

   Additionally, the promotion for the Service attempted to force users into entering into the Service in order to unblock their browsers (**Appendix C**).

   The Executive noted that notwithstanding the fact that the above marketing method was implemented by an affiliate marketer and not the Level 2 provider, the Level 2 provider was wholly responsible for the content of promotional material used to market the Service by affiliate marketers.

   The Executive therefore asserted that consumers and/or any recipients who had their internet browser functionality impaired were not treated fairly and equitably.

   The Executive submitted that the Level 2 provider was in breach of rule 2.3.1 of the Code as

a result of the aggressive affiliate marketing for the Service, and accordingly, outcome 2.3 had not been satisfied.

2. The Level 2 provider stated that the UK:

> "[I]s a tiny market for us, our revenue has been declining every month and it is not profitable. It does not warrant any investment by our company in the resources required to manage the market."

It added that the websites referred to in the breach letter (which purported to advertise a "Wi-Fi Hack", "Fake Zynga Credits", "YouTube videos" etc.) are all third party websites. In fact, it was not aware of their existence until it read the breach letter. It added that there are millions upon millions of websites online, and any one of those websites could point a link to the Service website. It stated that it, "absolutely cannot control who links to its website".

It stated that it could stop payments to those with which it directly contracts, but that it is, "impossible for us to police every inbound link online. It is obvious some of these websites are a fraud, setup to defraud companies like ours."

The Level 2 provider added that the because of the lack of profitability and the:

> "[R]equirement for our company to take some responsibility for websites we have neither seen nor heard of, we made the decision to exit the UK market on 3rd July. This notification was passed via our advertising team to stop buying any UK advertising. This was sometime before your investigation."

It added that it had always responded to regulatory and compliance issues with speed. It had issued refunds to any customer who requested them and it had invested its time and resources.

During informal representations, the Level 2 provider stated that it began operation of the Service in the UK in June 2012 and that the UK was a small market for it. It asserted that its Service did not include the ransomware promotions and that affiliate marketers were difficult to police. It submitted that its Service was 100% complaint. Pricing was prominent and all the required messages were sent.

In relation to affiliate marketing, the Level 2 provider stated that affiliate networks work with hundreds of affiliates and that unscrupulous publishers use lots of methodologies to push traffic. It added that it appeared that ransomware had been linked to its Service and six competitors too. However, consumer harm had been minimal and that it had removed the offers before it had been contacted by PhonepayPlus. This was because the Service was not making enough profit and that, "a couple of thousand dollars a month was not worth it".

The Level 2 provider stated that it had not been linked to similar issues in the past. It commented that affiliate networks earned between $1 and $9 (USD) per referral. They control thousands of publishers who can drive traffic to websites. Anyone can be a publisher and many do not care if they scam consumers as it can be quite lucrative. As affiliate networks work with sub-affiliates they can be hard to control.

The Level 2 provider stated that in some countries it was enough that its landing pages were compliant. But that, "online is a kind of wild west" and that it had demonstrated issues with

affiliate marketing to a large Australian Mobile Network operator. It added that it was difficult to control affiliate marketing.

The Level 2 provider stated that the UK market had been a difficult market for it and that affiliates were highly paid for UK leads. It stated that it had a traffic light system for grading affiliate marketing and only worked with trusted high quality (green) networks in the UK and Australia. It works with four to five affiliate networks and meets with them three to four times a year. It withholds funds where promotions are found to be non-complaint and makes affiliate marketers aware of the compliance required. The issue is that offers can be brokered and re-brokered. URLs could change five to six times before a consumer lands on a service landing page. It stated that it only pays out to one affiliate network, but that it could pay out to multiple networks and that there could be huge numbers in the chain.

It stated that it had a number of checks and balances in place, these include:

1. Contracts with affiliate networks.
2. Prohibition on the use of certain networks.
3. Active daily monitoring.
4. Competitor analysis.

It accepted that there had been two subscriptions as a result of the ransomware affiliate marketing (including the RMIT).

3. The Tribunal considered the evidence and submissions before it. The Tribunal commented that Level 2 providers are responsible for the operation of their services which includes the promotion of a service. Therefore, where a Level 2 provider chooses to engage in affiliate marketing, it accepts the risk that any affiliate marketing outside its direct control may lead to non-compliance for which it is responsible. Consequently, and for the reasons given by the Executive, the Tribunal concluded that consumers had not been treated fairly and equitably as a result of the malware affiliate marketing promotion in breach of rule 2.3.1 of the Code. 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 acted in breach of rule 2.3.2 of the Code as users were likely to have been misled into using the subscription Service and thereby incurred premium rate charges.

The Executive noted that the Level 2 provider is responsible for the content of promotional material used to market the Service by affiliate marketers.

Guidance

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

Paragraph 3.2

> "PhonepayPlus expects that all promotions must be prepared with a due sense of responsibility to consumers, and promotions should not make any factual claims that cannot be supported with evidence, if later requested by PhonepayPlus to do so."
>
> Paragraph 3.11
> "No promotion, with particular emphasis on SMS- or MMS-based promotion, should imply that the consumer will be making a one-off purchase, when they will, in fact, be entered into a subscription, or mislead the consumer as to the service they are being invited to purchase."
>
> Paragraph 3.12
> "An example of this would be a service that advertised itself as an 'IQ test' or 'love match', where the consumer was then invited to text or click to obtain more in-depth results, only to find that these results carry a further charge, or enter the consumer into an unwanted subscription."

The Executive asserted that consumers were misled or were likely to have been misled into entering the Service as a result of affiliate marketing that:

i. contained a large number of misleading statements;
ii. was likely to have misled users into downloading malware; and
iii. was likely to have misled consumers into the belief that they had to enter the Level 2 provider's Service at a cost of up to £4.50 per week In order to "unblock" their internet browser.

Reason 1: Users were misled into entering the Service as a result of ransomware affiliate marketing that utilised malware to lock consumers' internet browsers

The Service was promoted via affiliate marketing. The RMIT monitored the Service. The monitoring demonstrated that users were led into the Service via affiliate marketers, who introduced malware to the users' computer device (full details of the monitoring is contained in the "Background" section).

The Executive asserted that the user was led to believe they were required to complete a survey in order to download the Wi-Fi hacking software (**Appendix C**). Having clicked "Download" the user received a "WARNING!" notification informing them that the content viewed had been "blocked" and in order to "unblock" the content, s/he was required to complete at least one "offer. However, on selecting one of the offers, the user was directed to one of the Level 2 provider's Service landing pages and, whether the user interacted with the Service or not, the browser remained blocked.

The Executive noted that the Level 2 provider is responsible for the content of promotional material used to market the Service by affiliate marketers.

Further, the Executive asserted that users were highly likely to have been misled into landing on the Service website and interacting with the premium rate service as a result of being informed that they had to complete a survey to unblock their internet browser as their actions had been marked as that of a "spam bot".

The RMIT's monitoring evidence showed that, had an end user actually selected the "offer" (and entered the Service) the end user's internet browser would have remained blocked and automatically rerouted to the list of "offers" in an attempt to entice the end users to opt into

another premium rate service. The Executive accordingly asserted that this was highly likely to have misled consumers as they would have been under the impression that, by entering into a further premium rate service, their internet browsers would eventually be "unblocked".

Further, the Executive asserted that users were highly likely to have been misled into landing on the Service website and interacting with the premium rate service as a result of being informed that they had to complete a survey to unblock their internet browser as their actions had been marked as that of a "spam bot".

In light of the above the Executive further submitted that the Level 2 provider had acted in breach of rule 2.3.2 of the Code as a result of misleading affiliate marketing for the Service.

Reason 2: Users were misled into entering the Service as a result of other forms of affiliate marketing

Fake free unlimited Zynga Poker coins

On 29 April 2013, the RMIT monitored the Service and discovered it was promoted by affiliate marketers. The RMIT searched for "free coins" on Twitter and located a tweet that purported to offer free Zynga Poker chips. Zynga Poker is a popular virtual gambling game that can be played in Facebook. The RMIT clicked on the link within the tweet and was taken to a number of screens before one screen indicated that a survey needed to be completed before the download was complete. The RMIT selected the option "Chance to Win the All New iPhone 5" and was directed to the Level 2 provider's Service landing page. The RMIT did not subscribe to the Service.

The Executive asserted that the offer of free Zynga Poker coins was fake and the affiliate marketing campaign was a misleading inducement to encourage consumers to sign up to a premium rate service. The Executive further asserted that consumers would have been misled by the Zynga Poker campaign as it was highly likely that a consumer would have been led to believe that, by entering into the premium rate service, s/he would eventually obtain the coins.

In light of the above the Executive further submitted that the Level 2 provider has acted in breach of rule 2.3.2 of the Code as a result of misleading affiliate marketing for the Service.

Reason 3: Users were misled into entering the Service as a result of other forms of affiliate marketing

YouTube

On 30 April 2013, the RMIT monitored the Service. The RMIT searched for free Zynga Poker Chips in the Google search engine. The RMIT clicked on a link and was redirected to a video on YouTube. The RMIT clicked on a comment underneath the video, which seemed to offer free Zynga poker coins. The RMIT followed the link and was led through several webpages. A pop-up appeared with a list of offers that purported to unlock the download. The RMIT selected, "Win the new iPad Mini," and upon doing so, was directed to the Level 2 provider's Service landing page. On this occasion the RMIT did not sign up for the Service.

The Executive asserted that the offer of free Zynga Poker coins were fake and the affiliate marketing campaign was a misleading inducement to encourage consumers to sign up to a premium rate service. The Executive further asserted that consumers would have been

misled by the Zynga Poker campaign as it was highly likely that a consumer would have been led to believe that, by entering into the premium rate service, s/he would eventually obtain the coins.

In light of the above the Executive further submitted that the Level 2 provider has acted in breach of rule 2.3.2 of the Code as a result of misleading affiliate marketing for the Service.

2. The Level 2 provider relied on its submissions set out in relation to the breach of rule 2.3.1 of the Code.

3. The Tribunal considered all the evidence and submissions before it. The Tribunal commented that Level 2 providers are responsible for the operation of their services, which includes the promotion of a service. Therefore, where a Level 2 provider chooses to engage in affiliate marketing, it accepts the risk that any affiliate marketing outside its direct control may lead to non-compliance for which it is responsible. Consequently, and for the reasons set out in Reason 1, the Tribunal concluded that, as a result the misleading statements contained within the affiliate marketing promotions for the Service, consumers were likely to have been misled into believing that entering the Service would "unblock" their internet browsers. The Tribunal concluded that there had been a breach of rule 2.3.2 of the Code. Accordingly, the Tribunal upheld a breach of rule 2.3.2 of the Code.

Decision: UPHELD

ALLEGED BREACH 3

Rule 2.5.5

Premium rate services must not induce and must not be likely to induce an unreasonable sense of fear, anxiety, distress or offence.

1. The Executive submitted that the Level 2 provider had acted in breach of rule 2.5.5 of the Code as the marketing for the Service was likely to have induced an unreasonable sense of fear, anxiety, distress and/or offence to users as a result of:
   i. Users' internet browsers being compromised by ransomware; and/or
   ii. The language used in:
   a. The "Warning" pop up; and
   b. Having entered a PRS (and therefore taking the "required" actions to unblock their internet browsers), users being warned that:

      "This website has been blocked because of your recent activity. Your actions have been marked as a spam bot like, to visit this website again follow the instructions on the left. This is made for security reasons."

Monitoring

The Executive relied on the monitoring of the Service set out in the "Background" section above.

The Executive noted that the Service was promoted using affiliate marketing. As set out in the "Background" section, the Level 2 provider is responsible for the content of all promotional material used to market the Service.

The RMIT's monitoring demonstrated that users were led into the Service via affiliate marketers after having introduced malware to the consumers' computer device.

Users' internet browsers were blocked by malware

The Executive asserted that users who had been affected by the malware would have experienced a sense of fear, anxiety, distress and/or offence as, because of their actions, they had caused malware to be downloaded that compromised their computer. Further fear, anxiety, distress and/or offence was then likely to be caused by the fact that, despite following the instructions to unblock their browser, the browser continued to be compromised. At this point, the user was likely to have no idea how to rectify the situation and unblock their computer.

The language used in the "Warning" pop-up (Appendix C)

The Executive further asserted that the language used in the pop-up, which communicated the blocking of the browser, was likely to have induced an unreasonable sense of fear, anxiety, distress and/or offence to the recipients. Specifically, the pop-up that was forced upon the users stated "WARNING!" (in a large, red, bold font). In addition, it stated that, "The content you are browsing is blocked!" The use of this language, which informed consumers that their computer functionality had been impaired, was likely to have induced an unreasonable sense of fear, anxiety, distress and/or offence.

Additionally, end users who understood that their internet browser had been infected with malware would have been likely to have experienced fear, anxiety, distress and/or offence as they may have believed that their desktop security, including access to personal data and contacts, had been compromised.

The "spam bot" warning (Appendix B)

The Executive further asserted that the following statement was likely to induce fear, anxiety, distress and/or offence:

> "This website has been blocked because of your recent activity. Your actions have been marked as a spam bot like, to visit this website again follow the instructions on the left. This is made for security reasons."

The above statement accused consumers of engaging in "spam bot like" activity which suggested that consumers may have either acted unlawfully or had otherwise engaged in some form of unauthorised activity online. The Executive accordingly asserted that consumers would have been induced into a sense of fear, anxiety, distress and/or offence as a result of this accusation.

The Executive therefore asserted that users and/or any recipients who were induced to enter the Service as a result of the malware set out above were likely to have been caused an unreasonable sense of fear, anxiety, distress and/or offence. The Executive submitted that the Level 2 provider acted in breach of rule 2.5.5 of the Code and outcome 2.5 had not been satisfied.

2. The Level 2 provider relied on its submissions set out in relation to the breach of rule 2.3.1 of the Code.

3. The Tribunal considered all the evidence and submissions before it. The Tribunal commented that Level 2 providers are responsible for the operation of its services, which includes the promotion of a service. Therefore, where a Level 2 provider chooses to engage in affiliate marketing, it accepts the risk that any affiliate marketing outside its direct control may lead to non-compliance for which it is responsible. Consequently, and for the reason given by the Executive, the Tribunal concluded that consumers were likely to have been induced into an unreasonable sense of anxiety and distress in breach of rule 2.5.5 of the Code. Accordingly, the Tribunal upheld a breach of rule 2.5.5 of the Code.

Decision: UPHELD

ALLEGED BREACH 4

Rule 2.2.2

All written information which is material to the consumer's decision to purchase a service must be easily accessible, clearly legible and presented in a way which does not make understanding difficult. Spoken information must be easily audible and discernible

The Executive submitted that the Level 2 provider acted in breach of rule 2.2.2 because consumers were not fully and clearly informed of important operational terms before entering into the Service and that such information would have been material to a consumer's decision to purchase.

The Executive relied on the content of the Guidance on "Promotions and promotional material" and "Competitions and Games with other prizes".

Paragraph 2.13 Promotions and promotional material
"'Pricing information should be presented in a horizontal format and be easily legible in context with the media used. It should be presented in a font size that would not require close examination by a reader with average eyesight. In this context, 'close examination' will differ for the medium, whether on a static webpage, a fleeting TV promotion, in a publication, or on a billboard where you may be at a distance or travelling past at speed."

Paragraph 5.6 Promotions and promotional material
"Once on a webpage that promotes a PRS, consumers should not have to scroll down (or up) to view the key terms and conditions (especially, but not limited to, the price – see section 2 of this Guidance), or click on a link to another webpage. The PhonepayPlus Tribunal is likely to take the view that scrolling up or down to read key terms and conditions, or requiring the consumer to click on a link to view them, is in breach of Rule 2.2.5 of the PhonepayPlus Code of Practice."

Paragraph 5.7 Promotions and promotional material
"Level 2 providers should ensure that consumers do not have to scroll, regardless of screen resolution, to view the key terms and conditions of a service, or click on a link to view key terms and conditions. Key terms and conditions should be placed prominently on all website pages of the service that a consumer has to click through."

Paragraph 1.1 Competitions and Games with other prizes
"All promotional material should provide clear details as to how the competition operates.

Consumers must be made aware, before entering into the service, of any information that is likely to affect their decision to participate. Clear terms and conditions should include, but are not limited to:
•Information on any restrictions on number of entries or prizes that can be won;
•The incremental cost and the full cost of participation, where this is known".

Monitoring

The Executive relied on the monitoring of the Service carried out by the RMIT and detailed in the "Background" section. The Executive submitted that consumers were not clearly made aware of key terms and conditions at the outset. The Executive submitted the key information was as follows:

- confirmation that the Service is a subscription service;
- pricing;
- details of how to leave the Service;
- notice of other possible mobile network related costs;
- the dates for the quiz competition which spans across 15 months;
- the method of announcement of prize winners;
- the nature of the subscription service;
- handset specification requirements;
- eligibility and age restriction criteria; and
- the Level 2 provider's contact details.

The Executive asserted that the above key information was not easily accessible, clearly legible or presented in a way which did not make understanding difficult (**Appendices D and E**), because:

a. the key information, save for the first four bullet points above, appeared below the fold on the Service landing pages;
b. the terms and conditions were presented in a very small font and required close examination.
c. the terms and conditions failed to inform consumers of the number of prizes on offer.

Consequently the Executive submitted that the Level 2 provider acted in breach of rule 2.2.2 of the Code as consumers were not fully and clearly informed of key information likely to influence the decision to purchase prior to entering the Service.

2. During informal representations, the Level 2 provider stated that information appeared below the fold as a result of the RMIT's screen resolution and the number of toolbars displayed (three). It asserted that, "everyone pushes the terms and conditions below the fold," and that it was difficult to know how many toolbars users had. It added that, "yes we could make the window smaller," but that it would, "lose some real estate". It added that compliance was difficult as there was no prescriptive standard for screen size in the UK (unlike in Australia). It asserted that those who download toolbars expose themselves to adware and malware. Further, it added that it understood the Executive's concern regarding the "white space" between the terms and conditions and the call to action, but that it used a standardised template but this could be amended to make it smaller.

3. The Tribunal considered the evidence before it. The Tribunal noted that the key terms material to a consumer's decision to purchase were separated from the method of entry to the Service by a large white space on two of the Level 2 provider's Service web pages. The

Tribunal questioned whether the space had any purpose other than to push the key terms further down the page. In addition, the Tribunal noted that although consumers received a free message, which contained some key terms, a consumer could enter the Service without viewing the message. The Tribunal did not consider that the number of toolbars (three) displayed on the RMIT's screenshots was unusually high and therefore it did not accept the Level 2 provider's submission that some of the key terms appeared below the fold as a result of the number of toolbars displayed on the RMIT's screenshots. Finally, the Tribunal noted that the font size of the terms at the bottom of the pages was very small. Accordingly, the Tribunal concluded that all written information material to the consumer's decision to purchase was not easily accessible and clearly legible and upheld a breach of rule 2.2.2 of the Code.

Decision: UPHELD

SANCTIONS

Initial Overall Assessment

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

Rule 2.3.1 – Fair and equitable treatment

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

☐
- Very serious cases have a clear and highly detrimental impact, directly or indirectly, on consumers.
- The nature of the breach, and/or the scale of potential harm to consumers, is likely to severely damage consumer confidence in premium rate services.
- The nature of the ransomware was such as to cause distress and/or anxiety and/or take advantage of a consumer who is in a position of vulnerability.
- The scam promotion constitutes fundamental non-compliance with the Code.

Rule 2.3.2 - Misleading

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

☐
- Very serious cases have a clear and highly detrimental impact, directly or indirectly, on consumers.
- The nature of the breach, and/or the scale of potential harm to consumers, is likely to severely damage consumer confidence in premium rate services.
- The nature of the ransomware was such as to cause distress and/or anxiety and/or take advantage of a consumer who is in a position of vulnerability.
- The scam promotion constitutes fundamental non-compliance with the Code.

Rule 2.5.5 - Avoidance of harm (fear, anxiety, distress and/or offence)

The initial assessment of rule 2.5.5 of the Code was **very serious**. In determining the initial assessment for this breach of the Code the Tribunal applied the following criteria:

☐
- Very serious cases have a clear and highly detrimental impact, directly or indirectly, on consumers.
- The nature of the breach, and/or the scale of potential harm to consumers, is likely to severely damage consumer confidence in premium rate services.
- The nature of the ransomware was such as to cause distress and/or anxiety and/or

take advantage of a consumer who is in a position of vulnerability.

- The scam promotion constitutes fundamental non-compliance with the Code.

Rule 2.2.2 - Written material key to the decision to purchase

The initial assessment of rule 2.2.2 of the Code was **significant**. In determining the initial assessment for this breach of the Code the Tribunal applied the following criterion:

☐ • The Service was recklessly promoted in such a way so as to impair the consumer's ability to make a free and informed transactional decision.

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

Final Overall Assessment

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

- The Level 2 provider failed to follow Guidance in relation to pricing on some of its landing pages.
- There have been a significant number (approximately 11) of prior adjudications concerning affiliate marketing.
- The Level 2 provider benefited and/or would have potentially benefited from fraudulent marketing.

In determining the final overall assessment for the case, the Tribunal took into account the following mitigating factors:

- The Level 2 provider stated that it had the following measures in place to identify and mitigate against the risks associated with affiliate marketing:
  - Contracts with affiliate networks.
  - Prohibition on the use of certain networks.
  - Active daily monitoring.
  - Competitor analysis
- On being notified of the ransomware affiliate marketing, the Level 2 provider:
  - Launched an investigation.
  - Blocked the responsible affiliate network.
- The Level 2 provider asserted that it had made the decision to suspend the Service (for reasons unrelated to the ransomware promotions) prior to receiving notification from PhonepayPlus).

The Tribunal noted the measures that were taken by the Level 2 provider to control and monitor the risks posed by the use of affiliate marketing but commented that more could still be done to seek out rogue sites in a proactive manner.

Further, the Tribunal took into account the detriment suffered by the Level 2 provider as a result of the use of the Emergency procedure.

The Tribunal noted the Level 2 provider's assertion in relation to the limited number of leads generated from the ransomware promotion, which it said were just two, one of which was the RMIT. The Level 2 provider's relevant revenue in relation with the Service was in the range of Band 4 (£50,000 - £100,000).

The Tribunal noted that the Service and the Level 2 provider's landing pages were not predicated on fraudulent activity, that the Service had some value and that a large part of the Level 2 provider's revenue appeared to be from legitimate sources. The Tribunal also commented that there had been little consumer harm as a result of swift regulatory action from PhonepayPlus. Having taken into account the aggravating and mitigating factors, the Tribunal concluded that the seriousness of the case should be regarded overall as **very serious.**

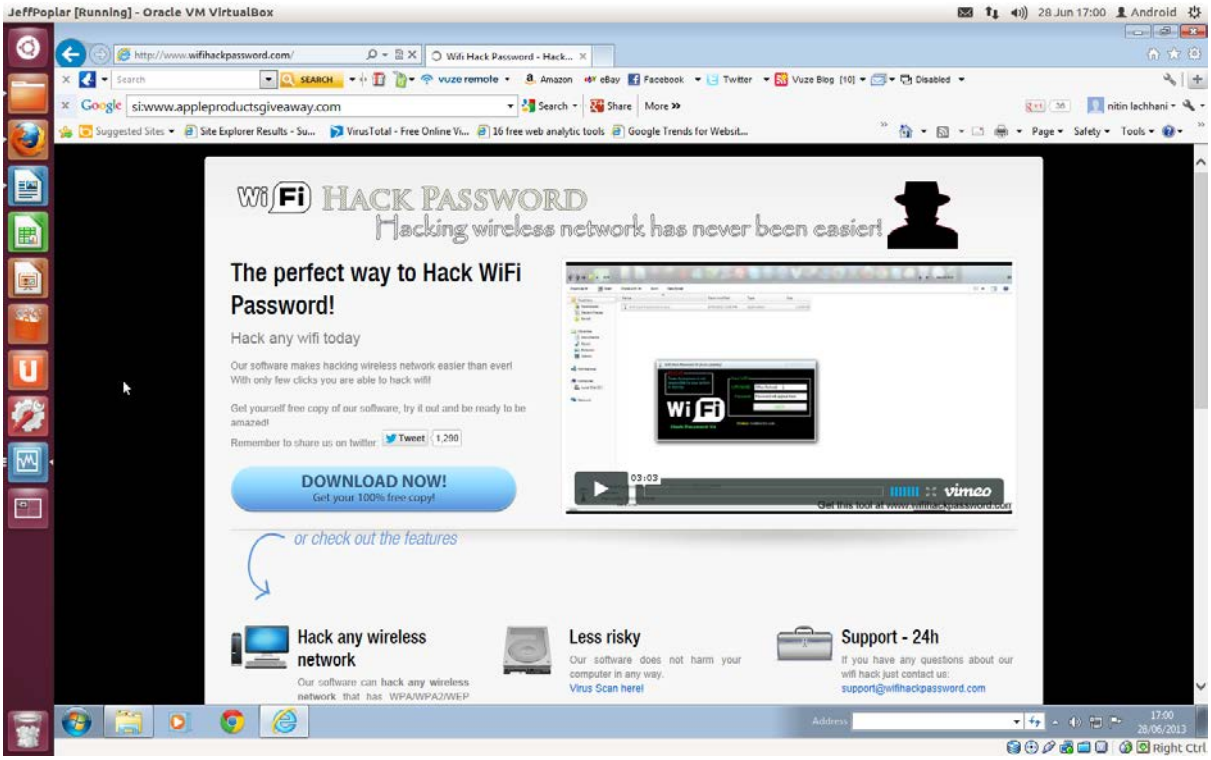
Sanctions Imposed

The Tribunal noted that the circumstances of the case were unusual as it was the first time that ransomware had been detected to have been used in the promotion of premium rate services. It also noted that there were no complaints regarding the ransomware promotions from consumers. Having regard to all the circumstances of the case, the Tribunal decided to impose the following sanctions:

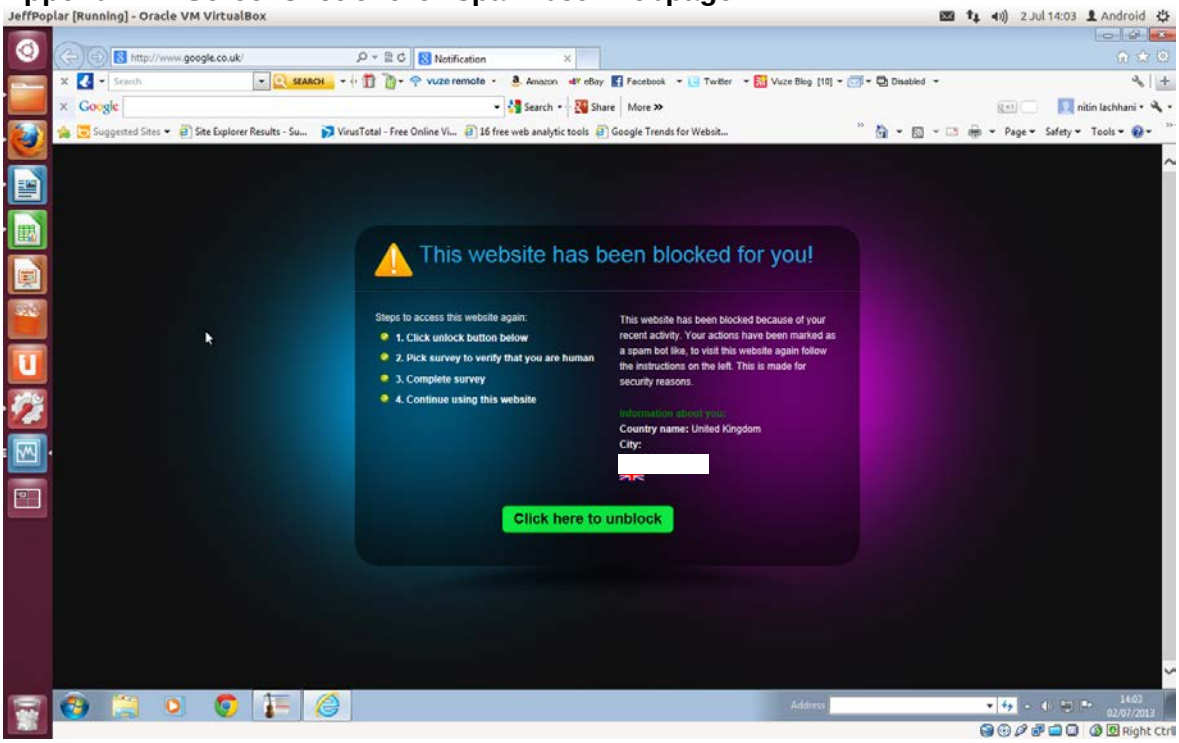
- a formal reprimand;
- a warning that if the Level 2 provider fails to ensure that it has sufficient measures in place to prevent actual or potential consumer harm being caused by affiliate marketing in future, it should expect to receive a significant penalty for any similar breaches;
- a fine of £25,000; 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

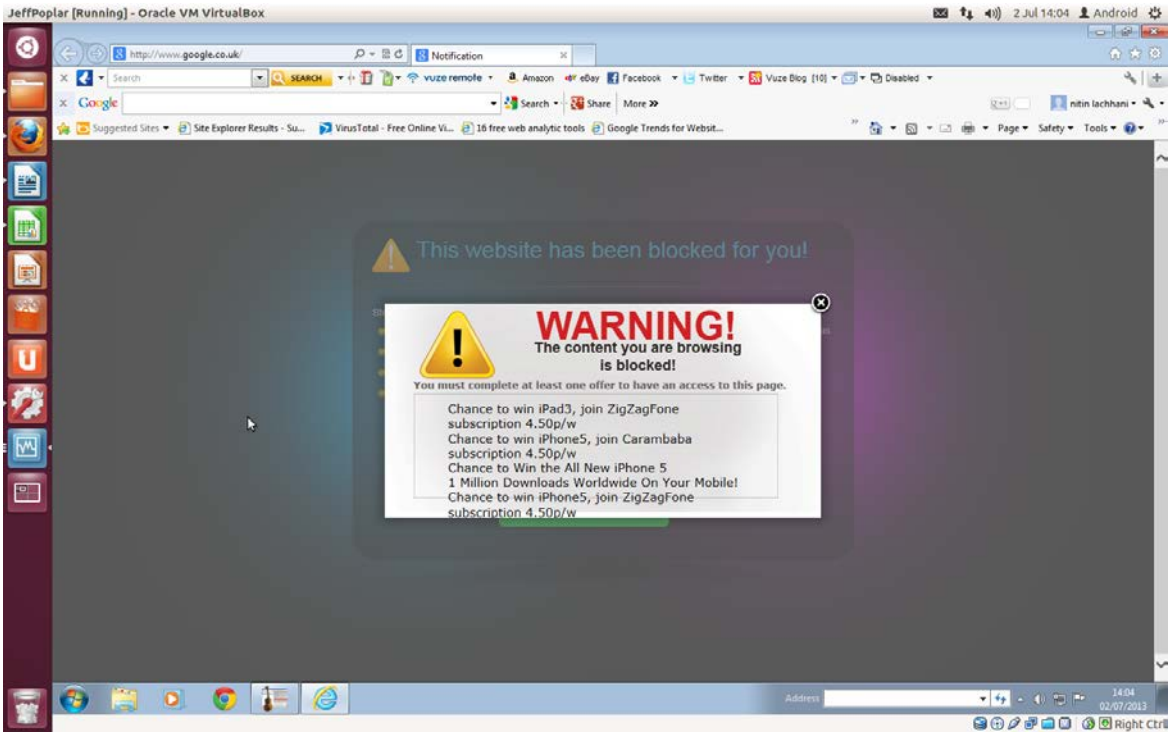
Appendix A: Screenshot of wifihackpassword.com:



Appendix B: Screenshot of the "spam bot" webpage:



Appendix C: Screenshot of the "Warning" webpage:



Appendix D: Screenshot of the Service "quizm8" webpage:

Appendix E: Screenshot of the Service "quizm8" means of entry webpage:

Appendix F: Screenshot of the Service "sms2win.me" landing page: