Tribunal Sitting Number 131 / Case 1

Case Reference: 28901

Level 2 provider	Hectiq B.V
Type of Service	Competition - non-scratchcard
Level 1 provider	Oxygen8 Communications UK Ltd
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, Hectiq B.V operated an online subscription mobile content and competition quiz service using the brand names "ZigZagFone" and "Carambaba" (the **"Service"**). The Service operated on the premium rate shortcode 88101 at a cost of £4.50 per week (three mobile terminating messages per week at £1.50) and was promoted via affiliate marketing. The Level 1 provider for the Service was Oxygen8 Communications UK Ltd.

The Service offered consumers the opportunity to receive mobile content that included wallpapers, ringtones and celebrity gossip. Consumers were also offered the opportunity to participate in quiz competitions. The consumer who answered the most questions correctly in the shortest time period during the competition period, won a prize, such as Apple products. The competition period was due to end on 31 December 2013.

The Service operated from 17 June 2013 to 8 July 2013 (when it was suspended as a result of the use of the Emergency procedure).

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 ("**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 and 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 a file 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 the RMIT was given was to click "OK". The RMIT noted from previous monitoring experiences that accepting the upgrade led it to the landing pages of a premium rate subscription service. Upon subscription to the service promoted, a password was "unlocked". However, the password had no function and no upgrade took place. The RMIT's internet browser was blocked by the malware and was not unblocked following entry into the subscription Service.

The RMIT conducted an additional monitoring session on 1 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 during the previous monitoring sessions, the RMIT clicked on the "Click here to unlock" button, and 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 an iPad 3, join ZigZagFone subscription 4.50p/w!" The RMIT was subsequently directed to the Level 2 provider's ZigZagFone landing page which opened in a new browser window **(Appendix D**).

The RMIT followed the instructions contained on the landing page and answered one multiple choice question. The RMIT was directed to enter its MSISDN and click "Confirm". The next screen prompted the RMIT to send the keyword "GAME" to the shortcode 88101 to opt-in to the Service. 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 messages that confirmed the RMIT had successfully opted-in to the Service.

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 that 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 finished the monitoring the session.

The RMIT conducted an additional monitoring session on 2 July 2013. The RMIT again opened the Internet Explorer browser and found it was still 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 second offer, "Chance to win iPhone5, join Carambaba subscription 4.50p/w," and was directed to the Level 2 provider's Carambaba landing page. The RMIT completed one multiple choice question and was then

prompted to enter its MSISDN and click "Continue" (**Appendix E**). The RMIT was then prompted to text the trigger keyword "PLAY" to the premium rate shortcode 88101. This was followed by subscription confirmation messages. The RMIT opted-in to the Service but the internet browser remained blocked.

During each 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.

In order to unblock its internet browser, the RMIT had to re-boot its desktop computer 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 were communicated to the Level 2 provider on 8 July 2013. The Level 1 provider was directed to withhold revenue on 8 July 2013. On 8 July 2013, the Level 2 provider confirmed that the Service had been suspended and on 10 July 2013, the Level 1 provider confirmed that the revenue payment had been withheld.

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.

On 10 July 2013 the Level 2 provider requested a review of the use of the Emergency procedure and/or the imposition of the suspension and withhold. On 12 July 2013 the Tribunal refused the application to terminate the use of the Emergency procedure and cease the (whole or part of the) withhold but agreed that the suspension could be lifted subject to the satisfaction of four conditions. The conditions were satisfied and access to the Service resumed on 2 August 2013.

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 or offence)
- 2.2.5 - Pricing prominence
- 2.2.2 - Written information material to the decision to purchase

The Level 2 provider responded on 30 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 ISSUE

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.

The Tribunal noted that the Level 2 provider asserted that the ransomware was not part of the promotion of the Service. However, the Tribunal found that the malware (ransomware) contained an inducement to enter the Service and therefore it formed part of the promotion for the Service.

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 it found the content of the RMIT's monitoring to be shocking and the method of marketing used was unacceptable and not approved by it. It added that it was aware of the risks involved with affiliate marketing and, as a result, it had strict procedures in place. It stated that the procedures include:

1. Strict rules for affiliate marketers and publishers.
   -The terms and conditions are part of the standard purchase order with an affiliate network. Affiliate partners are required to sign the terms and conditions prior to promoting the Service.
2. Country specific rules.
3. Prior approval of all third party marketing material.
4. Blacklisting non-compliant affiliates and publishers.
5. Monitoring of extraordinary increases in conversions or in complaints.

In addition, the Level 2 provider stated that because the UK is a sensitive market and as it was aware of the recent PhonepayPlus adjudications regarding affiliate marketing, it only worked with five selected affiliate partners in the UK in order to create maximum control. It asserted that its safeguards and procedures showed that it makes the maximum efforts that reasonably can be expected to ensure that affiliate networks and their publishers comply with all applicable rules and regulations. It added that it was therefore quite disappointed that, despite these safeguards and procedures, its services were still linked to the method of marketing described by the Executive in the breach letter.

The Level 2 provider submitted that it had tracked the non-compliant promotion and located the responsible publisher. It provided evidence that it had written to the publisher and intended to hold it to account. It added that it had ceased all promotion through the relevant affiliate network and that the ransomware promotion was only live from 1 July until 4 July 2013.

With regard to the Executive's claim that consumers and/or any recipients who had their internet browser functionally impaired were not treated fairly and equitably, the Level 2 provider stated:

> "The malware was not installed on a consumer's computer by clicking on a promotion of Hectiq's services but by a consumer actively visiting www.wifihackpassword.com and clicking on the button "Download now" to (presumably) download software to hack wifi passwords. Hacking wifi passwords is illegal and consumers clicking on the download button were attempting to download software for illegal purposes. As one can see from the screenshots in this official complaint, at the stage where the consumer clicked the download button and downloaded the malware there was not any promotion for Hectiq's services involved and/or mentioned yet. Although Hectiq obviously regrets that Hectiq's services were at a later stage linked to the (supposed) unblocking of the browser, at the first stage where the consumer downloaded the malware this was not the case yet. The fact that consumers downloaded the malware was not a consequence of a promotion of Hectiq's services, but a consequence of consumers wishing to obtain hacking software. Hectiq is of the opinion it cannot be held responsible for the results of consumers attempting to download software for illegal purposes."

Notwithstanding the above, the Level 2 provider requested that the Tribunal take into account that:

1. it had made the maximum efforts that reasonably could be expected of it to ensure that the affiliate networks and their publishers complied with all applicable rules and regulations;
2. the ransomware method of marketing had only been live for a very limited time.
3. no complaints were received from consumers;
4. given the low number of subscriptions, the number of consumers possibly affected by the ransomware marketing was limited;
5. it immediately voluntarily unsubscribed all 390 active subscribers on receipt of the Emergency procedure notification from PhonepayPlus; and
6. it had voluntarily offered all 390 customers a full refund of their charges in a sms message on 24 July 2013.

During informal representations, the Level 2 provider stated that the method of marketing was completely unacceptable. It stated that despite all safeguards, it was linked to the ransomware promotions. The incident was damaging to consumers, the affiliate networks and itself. It added that it had taken the maximum efforts to ensure compliance and did not see what else it could have done to avoid the non-compliance. It asserted that it would not pay the affiliate network responsible. It stated that it had a meeting scheduled with one of its affiliate marketing partners to discuss the incident and prevention of future occurrences. It had also organised an industry-wide meeting with five competitors on the issues "flooding the industry" regarding affiliate networks and content providers. The Level 2 provider stated that the incident would "hurt" publishers as there would be uncertainty as to whether they would be paid.

The Level 2 provider commented that the UK is a sensitive market with strict rules and regulations. It added that to ensure compliance it:

i. pre-approved marketing.
ii. conducted monitoring (carried out by its marketing and legal teams). However, it added that it could only "go as deep" as partner level. It added that it paid particular attention to out of trend conversions. Where conversions are high, it requests proof of promotion from the responsible affiliate network.
iii. had in-house customer care (including investigating peaks in traffic).
iv. had constant contact with the Level 1 provider and PhonepayPlus contacts.
v. had agreements with affiliate networks, which include the "rules of play".
vi. blocked non-compliant traffic.

vii. completed compliance check by the Level 1 provider on every service.
viii. conducted bi-monthly compliance meetings.

It asserted that it took more steps than its competitors. However, it accepted that it could check web forums and blogs more.

The Level 2 provider commented that all consumers are worthy of protection but that the average consumer was aware of the risks of downloading illegal hacking software. It added that consumers should not be misled into using any service.

In relation to the Service, it stated that there were 390 consumers in total. It asserted that it had unsubscribed all the consumers as it would have been difficult to identify how individual consumers were led to the Service (as further down the affiliate marketing chain there was less of a willingness to give names and/or other information). It stated that in theory all the subscribers could have been led into the Service as a result on non-compliant promotions, but that this was unlikely. However, to be sure, and in light of the low number of subscribers, it had decided to unsubscribe all the subscribers.

In conclusion, the Level 2 provider stated that providers would only survive without affiliate marketing if all providers ceased using affiliate marketing. It asserted that it was developing its own direct marketing tool but that it was not live yet. Further, it was not sure that affiliate marketing needed to be stopped entirely, but that it was not going to allow anyone to promote its services and "watch from a distance".

3. The Tribunal considered the evidence and submissions before it. The Tribunal noted that the Level 2 provider accepted that the affiliate marketing promotions were in breach of rule 2.3.1 of the Code. 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 Service and thereby incurred premium rate charges.

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.

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:

"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."

"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."

"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."

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 file (**Appendix B**). 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 selected the "offer" (and entered the Service), the end user's internet browser would have remained blocked and automatically re-routed 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".

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.

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

In addition, the Level 2 provider stated that it disagreed that the promotion for the Service was likely to have misled users into downloading malware. It commented that the malware was not installed on a consumer's computer by clicking on promotions for the Service but by a consumer actively visiting www.wifihackpassword.com and clicking on the button "Download now" to (presumably) download software to hack Wi-Fi passwords. The Level 2 provider commented that hacking Wi-Fi passwords is illegal and consumers clicking on the download button were attempting to download software for illegal purposes. It added that, "As one can see from the screenshots in this official complaint, at the stage where the consumer clicked the download button and downloaded the malware there was not any promotion for the Service."

It stated that it obviously regretted that the Service was at a later stage linked to the (supposed) unblocking of the browser. However, at the first stage where the consumer downloaded the malware this was not the case. It asserted that the fact that consumers downloaded the malware was not a consequence of a promotion of the Service, but a consequence of consumers wishing to obtain hacking software.

The Level 2 provider accepted that the assertions contained in the affiliate marketing promotions were misleading and that they were likely to have misled consumers into the belief that they had to enter the Service in order to unblock their internet browser at a cost of £4.50 per week. It added that it obviously very much regretted that, despite all the safeguards and procedures it had incorporated in relation to affiliate marketing, the Service was still linked to this misleading method of marketing.

3. The Tribunal considered all the evidence and submissions before it. The Tribunal noted that the Level 2 provider accepted that the affiliate marketing promotions were in breach of rule 2.3.2 of the Code. 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, 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.

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 submission set out in relation to the breach of rules 2.3.1 and 2.3.2 of the Code.

   In addition, the Level 2 provider accepted that the downloading of the malware might have induced or was likely to induce an unreasonable sense of fear, anxiety, distress or offence. However, it stated that the malware was not installed on a consumer's computer by clicking on a promotion of the Service but by a consumer actively visiting www.wifihackpassword.com and clicking on the button "Download now" to (presumably) download software to hack Wi-Fi passwords.

   With regard to the "spam bot" pop-up, it commented that at that stage there was no promotion for the Service involved and/or mentioned. Furthermore, it added that although it strongly condemned the use of malware and the method of marketing used, it stated that hacking Wi-Fi passwords is illegal, and that consumers clicking on the download button were attempting to download software for illegal purposes.

   Finally, the Level 2 provider stated that the "Warning" pop-up was where the Service was first mentioned, and that it obviously very much regretted that, despite all the safeguards and procedures it had incorporated in relation to affiliate marketing, the Service was still linked to this misleading method of marketing.

3. The Tribunal considered all the evidence and submissions before it. The Tribunal noted that the Level 2 provider accepted that the affiliate marketing promotions were in breach of rule 2.5.5 of the Code. 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, the Tribunal concluded that consumers were likely to have been induced into an unreasonable sense of anxiety and distress by the "WARNING!" pop-up which promoted the Service.

Accordingly, the Tribunal upheld a breach of rule 2.5.5 of the Code.

Decision: UPHELD

ALLEGED BREACH 4

Rule 2.2.5

In the course of any promotion of a premium rate service, written or spoken or in any medium, the cost must be included before any purchase is made and must be prominent, clearly legible, visible and proximate to the premium rate telephone number, shortcode or other means of access to the service.

1. The Executive asserted that the Level 2 provider acted in breach of rule 2.2.5 of the Code because pricing was not prominent and proximate to the means of access on some of the promotional landing pages for the Service.

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

   Paragraph 2.2
   "As a starting point, 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. be unlikely to cause confusion)."

   Paragraph 2.8
   "Pricing information where consumers are unlikely to see it, or where it is hard to find, is unlikely to be judged as 'prominent', or 'proximate', by a PhonepayPlus Code Compliance Panel Tribunal ('PhonepayPlus Tribunal')."

   Paragraph 2.10
   "Lack of prominence, or proximity, most often takes place online (both web and mobile web), where the price is provided in small print elsewhere on the page from the call to action. We have sometimes seen pricing information in the middle of the terms and conditions of a service, promotion or product, rather than as clear and correct 'standalone' information; the price is sometimes provided separate from the page with the call to action, or lower down on the page in such a way as to make the consumer have to scroll down to see the price. Any of these practices are unlikely to be viewed as compliant with PhonepayPlus' Code of Practice by a PhonepayPlus Tribunal."

   The Executive noted that during the in-house monitoring on 2 July 2013 two screenshots belonging to the Carmababa service were viewed. Generally, the Executive noted that most of the Service landing pages contained pricing information. However, it was in a small font size particularly in comparison to the large multi-coloured wording that described the prize. Further, on the page that required the user to enter their MSISDN, the small pricing information was not standalone and some distance from the "CONTINUE" button, which was fully capitalised and highlighted in red. **(Appendix E and F)**.

   The Executive submitted that throughout the promotional material, attention was drawn towards the product and/or the means of access to the Service, which often overshadowed the pricing information.

   As a result of the reasons set out above, the Executive submitted that the Level 2 provider had acted in breach of rule 2.2.5 of the Code.

2. The Level 2 provider stated that it had been asked by a Mobile Network operator to revise its pricing information and that it had already addressed this matter by revising the pricing. It stated that it always turns around changes within a day.

3. The Tribunal considered the evidence and the submissions before it. In relation to the Service landing page at **Appendix F**, the Tribunal found that although pricing information was displayed twice, it was too small and therefore could not be considered to be sufficiently prominent. The Tribunal noted that clear pricing information was contained in SMS messages sent to the consumers, but that this was irrelevant as consumers could enter the Service without viewing the messages. Accordingly the Tribunal upheld a breach of rule 2.2.5 of the Code.

Decision: UPHELD

ALLEGED BREACH 5

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.

1. 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'.

   Paragraph 2.13
   "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 2.14
   "The use of colour (see immediately below) also needs to be considered, as this could affect the need for close examination, regardless of font size."

   Paragraph 2.15
   "There are a number of instances when the combinations of colours used in promotional materials reduces the clarity of information and the ease with which is can be seen. Providers should take care to ensure that the colour combinations (including black on white) used for the presentation of the price do not adversely affect the clarity."

   Paragraph 5.7
   "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."

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. The Executive submitted the key information was as follows:

- pricing;
- details of how to leave the Service; and
- partial customer service details for the Level 2 provider.

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 (**Appendix G**), because;

a. full information material to a consumer's decision to purchase and enter the premium rate service was presented below the fold within the Service landing page.
b. the terms and conditions were presented in a small font size and required close examination.

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. The Level 2 provider stated that all its pages are scripted for the most commonly used screen resolutions. However, if a computer has a small resolution or if the personal settings of the user contain a lot of toolbars scrolling may be required to see all the text. For example, the RMIT's screenshots showed that the page was pushed down because of the multiple toolbars used. It added that, since the pages were built for the most commonly used screen resolution, it was convinced it had displayed everything correctly in at least 95% of cases. It commented that because of the personal settings of some users, it is technically impossible to serve 100% of consumer's screens.

   During informal representations, the Level 2 provider stated that whether terms and conditions appeared above the fold depended on screen size and the number of tool bars displayed. It asserted that it had started working on a project to ensure that all content is displayed without the requirement to scroll down irrespective of screen size.

3. The Tribunal considered the evidence and submissions before it. The Tribunal commented that it considered that the breach was "borderline" as the key information contained on the Service landing pages was small and at times partly below the fold. However, the Tribunal noted that the key information material to consumers' decision to purchase was more clearly displayed on other Service landing pages and in the free SMS messages sent to consumers prior to purchase. Therefore, taking into account the Service as a whole, consumers were made aware of all material key to their decision to purchase prior to making a purchase. As a result the Tribunal did not uphold a breach of rule 2.2.2 of the Code. The Tribunal commented that it hoped that the Level 2 provider would voluntarily seek compliance advice from PhonepayPlus to improve the compliance of the Service landing pages. The Tribunal also added that it was pleased that the Level 2 provider was taking steps to implement responsive web design, which would result in pages being clearly visible on all devices and computers.

Decision: NOT 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 2.2.5 – Pricing prominence and proximity

The initial assessment of rule 2.2.5 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 could have taken additional steps to monitor affiliate marketing for the Service, including monitoring blogs and forums.
- 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:
  - Prescriptive country specific rules for affiliate marketing for the Service.
  - Limit to number of affiliate networks it contracted with.
  - Prior approval of marketing material.
  - Proactive monitoring of spikes.
  - Blocking non-compliant affiliate marketers and publishers.
  - Withholding payment from non-compliant affiliate partners.
- On being notified of the ransomware affiliate marketing, the Level 2 provider:
  - Blocked the responsible affiliate network.
  - Sent all subscribers a message offering a refund.
  - Notified the responsible publisher that it intended to take action against him.
  - Organised an industry meeting with its competitors to discuss affiliate marketing.
- The Level 2 provider provided full details of the publisher responsible for the ransomware promotions.

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 Level 2 provider's revenue in relation to the Service was in the range of Band 6 (£1 - £5,000).

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 from consumers. Having regard to all the circumstances

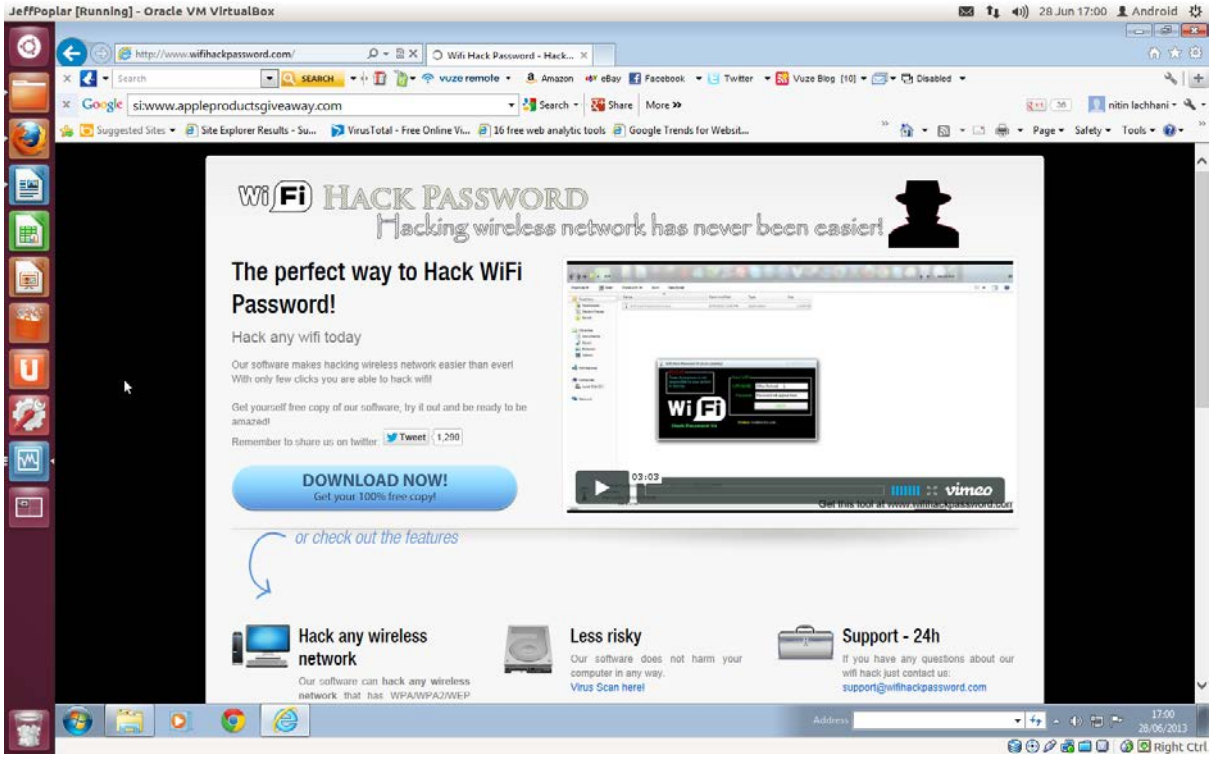
of the case, the Tribunal decided to impose the following sanctions:

- 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; and
- a fine of £23,000.

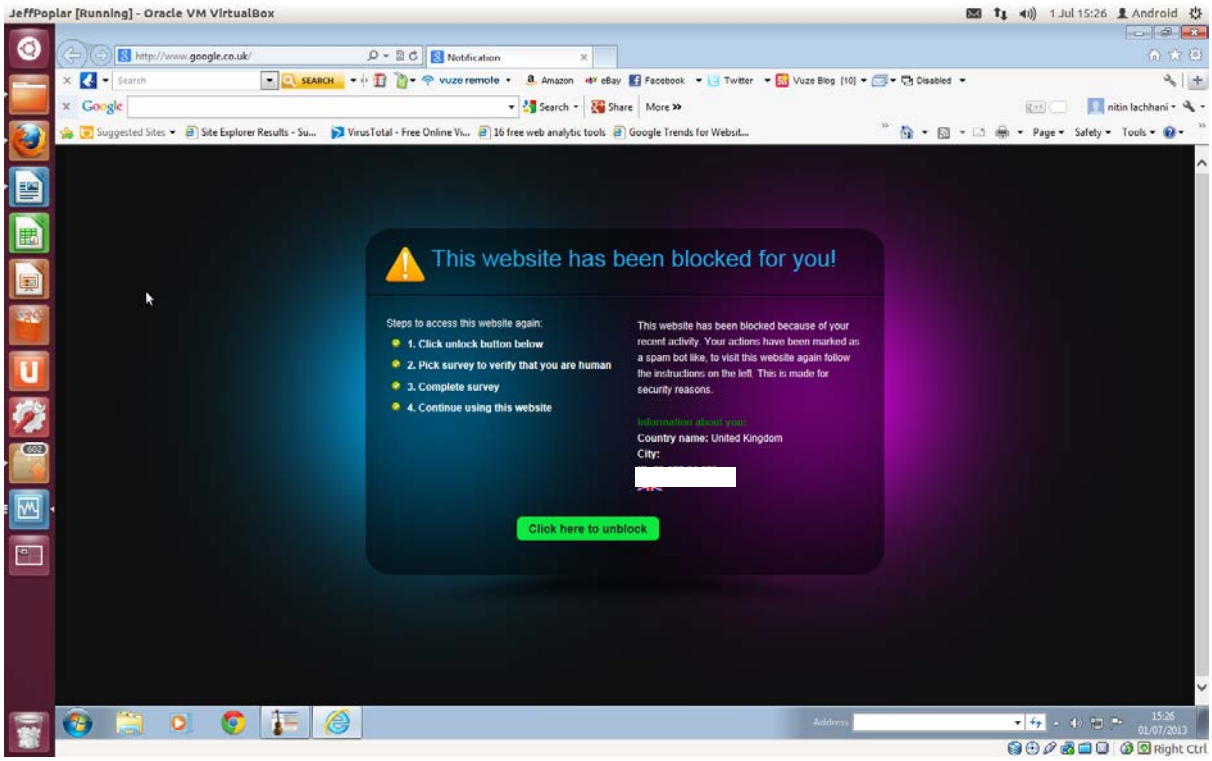
The Tribunal noted the steps taken by the Level 2 provider to refund consumers and concluded that it was not necessary to impose a refund sanction.

Appendices

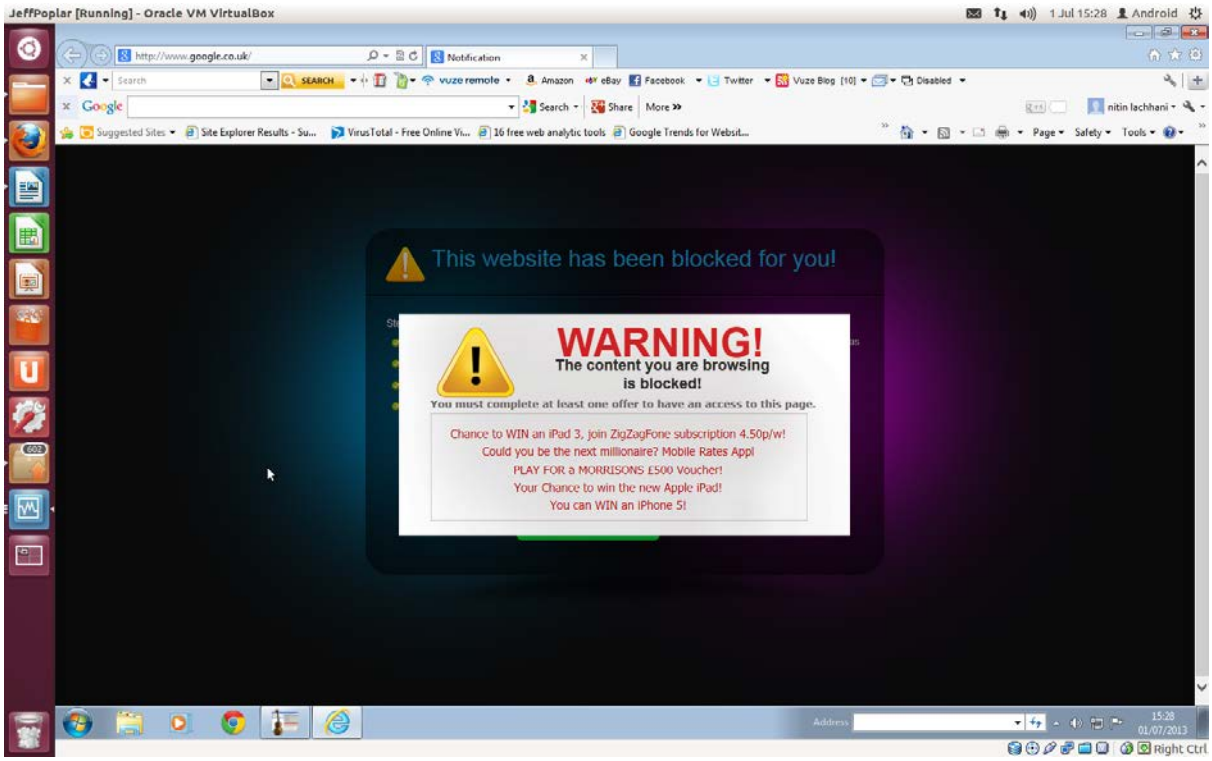
Appendix A: Screenshot of wifihackpassword.com:



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

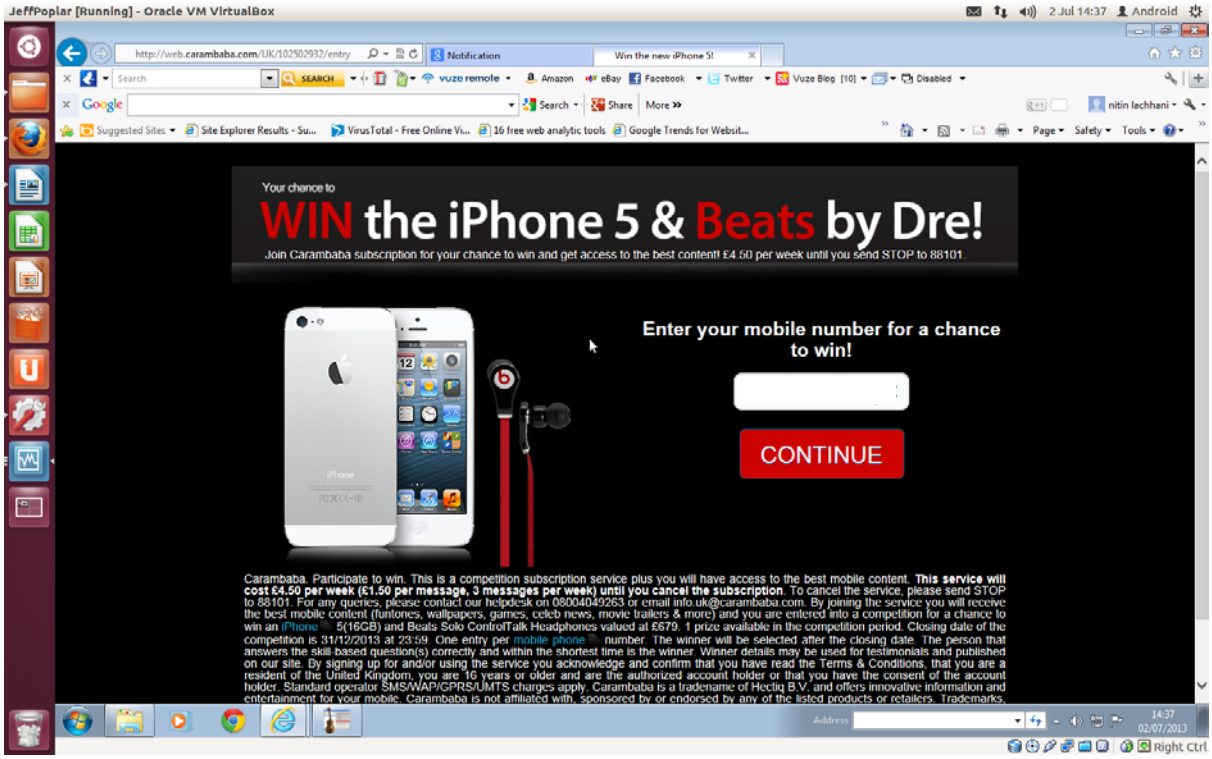


Appendix C: Screenshot of the "WARNING!" webpage:



Appendix D: Screenshot of the "Zigzagfone" Service landing page:

Appendix E: Screenshot of the "Carambaba" Service landing page:



Appendix F: Screenshot of a "Carambaba" Service webpage:

Appendix G: Further screenshot of a "Carambaba" Service webpage: