Code Compliance Panel

Tribunal Decision

Tribunal Sitting Number 136 / Case 1

Case Reference: 28903
Level 2 provider: Greenwhale Holding Ltd, Anguilla
Type of Service: Competition and mobile content (subscription)
Level 1 provider: Globway B.V and Oxygen8 Communications 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, Greenwhale Holding Ltd, operated an online subscription mobile content and competition service, using the brand name "Brickoffers" (the **"Service**"). The Service operated on the premium rate shortcode 82070 at a cost of £4.50 per week (three messages per week at £1.50 each) and was promoted via affiliate marketers. The Level 1 provider for the Service was Globway B.V. and Oxygen8 Communications Limited.

The Service offered consumers the opportunity to receive mobile downloads described as "funtones" and the opportunity to enter a prize draw to win an iPad. The winner of the iPad was due to be selected at the end of the competition period (which ran from 1 June 2013 to 1 December 2013).

The Service operated from 19 June 2013 to 9 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 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.

In addition, the Executive had concerns regarding the visibility of key terms. PhonepayPlus received one complaint regarding the Service. The complaint did not concern the ransomware promotion.

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. A dialogue box instantly 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 completion a password was unlocked which had no function and no upgrade took place. The RMIT's internet browser was blocked by malware contained in the download and was not unblocked following entry into the subscription Service.

The RMIT conducted an additional monitoring session on 3 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 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, "Mobile Content, Prizes, Downloads, Coupons & More!" The RMIT was directed to a webpage which purported to be the Service landing page which opened in a new browser window (**Appendix D**).

The RMIT followed the instructions contained on the landing page (http://funloadia.com) (**Appendix D**) and answered one quiz question. The RMIT was directed to enter its MSISDN and click "Continue". The next screen prompted the RMIT to send the keyword "READY" to the shortcode 82070 to opt-in to the Service (no pricing information was included in the message) (**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 messages that confirmed the RMIT had successfully opted-in to the Service.

The RMIT waited for the original password file that had been downloaded to become unlocked on the blocked browser tab, however this did not occur. The RMIT viewed the following statement:

> "WARNING! The content you are browsing is blocked! You must complete at least one offer to have access to this page…We are waiting for you to complete your survey. When you have completed the survey, please check back here to see if the content is unlocked. If you have spent more than 5 minutes on this survey and this page is still locked, please try a different survey…Not yet complete"

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 finished the monitoring the session.

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.

It is of note that in order to unblock its internet browser, the RMIT had to re-boot its 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 both the Level 1 and Level 2 provider on 8 July 2013. On 9 July 2013, both the Level 1 provider and the Level 2 provider confirmed that the Service had been suspended.

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

The Executive sent a breach letter to the Level 2 provider on 22 July 2013. Within the breach letter the Executive raised the following breaches of the Code:

- Rule 2.3.1 – Fair and equitable treatment
- Rule 2.3.2 – Misleading
- Rule 2.5.5 - Avoidance of harm (fear, anxiety, distress or offence)
- Paragraph 3.4.12(a) – Registration of numbers
- Rule 2.2.2 – Written information material to the decision to purchase

The Level 2 provider responded on 30 July 2013. On 8 August 2013, the Tribunal heard informal representations conducted on behalf of the Level 2 provider by a third party consultant. The Level 2 provider's representative clarified the Level 2 provider's written submissions. However, he was unable to answer some of the additional questions that arose. After careful consideration and in light of the nature of the Level 2 provider's response and further clarification, the Tribunal adjourned its consideration of the case to allow the Level 2 provider to submit evidence in support of its assertions, including, that there was no financial link between itself and the website through which the RMIT entered the Service (Funlodia).

Following the hearing, the Level 2 provider provided additional information to the Executive, which was considered by the Tribunal. On 17 October 2013, 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.

In addition, the Tribunal noted that the Level 2 provider asserted that its landing pages had been i-framed or scraped and placed without its knowledge on the Funlodia URL. Initially, the Level 2 provider asserted that it had no relationship with Funlodia. However, it later accepted that the seller ID of the publisher, who led the RMIT into the Service during the monitoring, belonged to one of the three affiliate marketing networks that it was directly contracted with. As a result, the Tribunal found that the use of the i-frame was merely a marketing technique used by a publisher who had a relationship with the Level 2 provider and would have expected to be remunerated for any leads to the Service.

Jurisdiction

The Tribunal noted that the Level 2 provider had reported the ransomware to the police on 24 July 2013 and had asserted that the matters raised by PhonepayPlus were criminal in nature and, although it supported PhonepayPlus in its regulatory objectives, it was not appropriate for it to be dealt with by PhonepayPlus. The Tribunal noted that PhonepayPlus had contacted the police and had provided information to them. The Tribunal held it was not precluded from adjudicating on the breaches that has been raised.

ALLEGED BREACH 1
Rule 2.3.1 Fairness
"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 denied that it had acted in breach of rule 2.3.1 of the Code and/or that it was responsible for any breach. The Level 2 provider stated that the Service was not the source of the malware. Instead, the source of the malware was the website wifihackpassword.com which it submitted was unsafe by its nature. It asserted that the website had "captured" the Service without the "slightest involvement by us".

The Level 2 provider stated that it did not regard the, "source of malware as 'marketing' or 'promotion'". It asserted that the use of malware was an illegal practice, as it was a form of cybercrime which harmed the integrity of (the promotion for) the Service, the Payforit scheme and the marketing program, by which bona fide affiliates were used.

The Level 2 provider submitted that:

> "[I]t should not and cannot be held responsible for an illegal deed of a stand-alone source which is unrelated ('The RMIT attempted to download a file containing a password to the premium rate services'), but appears to be related because of illegal access to our service. The particular source, by means one can illegally trespass the security of our service, could not be avoided as

our security measures are not immune for computer crime or cybercrime practices, as described."

In addition, the Level 2 provider submitted a detailed letter in which it expanded on its written submissions given in response to the breach letter. It stated that it had been successfully trading since 2009 and was "very distressed" to find its Service subject to the Emergency procedure. However, it stated that the Executive should have communicated its concerns in a more immediate manner as the delay between 28 June – 3 July and 8 July had resulted in the potential consumer harm being exacerbated and the Level 2 provider being prevented from conducting its own investigative research into the concerns. It submitted that had an urgent industry alert been proactively issued by the Executive, it would have placed industry on notice and allowed it to conduct its own urgent investigations. It had contracted with three affiliate networks, with thousands of publishers per network. Only one publisher was responsible for the ransomware and therefore "statistically approximately 95%" of consumers had entered the Service via compliant promotions.

Further, the Level 2 provider stated that under the twelfth edition of the Code, Level 2 providers were responsible for the actions of affiliate marketing promotions for their services. However it requested that the Tribunal consider in detail the general principles of law in relation to responsibility for criminal acts.

Generally, it added that the Executive appeared to have been confused in its submissions as its Service was "entirely unconnected" with Funlodia (the URL which appeared to host the Level 2 provider's landing pages during monitoring). It stated that its product URL was brickoffers.com.

During informal representations, a third party consultant acting on the Level 2 provider's behalf reiterated the Level 2 provider's written submissions. In addition the consultant stated that the Level 2 provider was based in the Dutch Antilles and was the smallest of the providers subject to the Emergency procedure in relation to the ransomware. It had three to four personnel, who had operated services for six/ seven years in other European countries. The consultant stated that the Service was live for testing from 19 June, but that marketing commenced on 25 June 2013. The Service was therefore trading for approximately 13 days prior to its suspension. The Level 2 provider was disappointed that it had not been alerted to the Executive's monitoring as soon as the ransomware was discovered. It was submitted that the Level 2 provider had carefully chosen its affiliate partners, had all necessary legal terms in place and that it had been very unfortunate to have got caught in the ransomware promotions on the first day of its operation.

The Level 2 provider was advised by its consultant to call the police E-Crime unit. It was submitted that the Level 2 provider understood its responsibilities but the situation was analogous to BT being held accountable for a nuisance call.

It was strongly asserted that the Service landing pages viewed by the RMIT in monitoring had been i-framed. It was submitted that the Level 2 provider had "no relationship" and "nothing to do with" Funlodia or similar services such as Loadia and that no money could have gone from the Level 2 provider to Funlodia. The genuine Service landing pages were hosted on a Brickoffers URL. The

consultant asserted that the genuine Service landing pages had been lifted off its site by what appeared to be an American company. The Level 2 provider does not operate in the USA. Further, it was stated that the customer service number on the i-framed page was not the Level 2 provider's which was "rather odd".

It was asserted that the Service had 673 subscriptions, all of whom, save for the RMIT, had entered the Service through a legitimate route. The Level 2 provider was contracted with three affiliate networks who led legitimate traffic to the Service landing pages. It was submitted that the Level 2 provider had done everything it could to control the affiliate marketing promotions for the Service, including monitoring for spikes, but that the data collected was very limited given that the Service was only live for a short time period.

Following the adjournment, the Level 2 provider provided further information in response to questions from the Executive. In particular, the Level 2 provider stated:

> "Investigations have been ongoing and since last week we can confirm that the statement of one subscriber via the malware route is incorrect. The figure is still very low as the traffic only ran from June 28th till July 9th. We now suspect that there were 69 unique MSISDN entry's of which 62 Opted-Out themselves within 24 hours after entering the service. [sic]"

In response to the question, "Please provide the full 'Seller ID' of the publisher who led the RMIT to subscribe to your service." The Level 2 provider provided the name of one of the three affiliate networks with which it was contracted.

In addition, the Level 2 provider accepted that the customer service number viewed by the Executive during monitoring was its Australian customer care number, which was incorrectly displayed on some of its UK disclaimer pages.

3. The Tribunal considered the evidence and submissions before it. In particular, the Tribunal noted the admissions made by the Level 2 provider in relation to the Seller ID of the publisher which led the RMIT into the Service and that it suspected that 69 consumers had been led to subscribe to the Service as a result of the ransomware. 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. As set out in the Background, the Tribunal noted that there was a nexus between the ransomware publisher and the Level 2 provider and therefore the Level 2 provider was responsible for the publisher's promotions for its Service. 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 blocking potentially 69 users internet browser functionality 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 Misleading
"Premium rate services must not mislead or be likely to mislead in any way.2

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 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 are 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 a page which purported to be 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".

In light of the above the Executive 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 the extensive submissions set out in response to the breach of rule 2.3.1 of the Code above.

   In addition and specifically in relation to the breach of rule 2.3.2 of the Code the Level 2 provider stated in its written submissions that the affiliate marketing did not result in the alleged breach of rule 2.3.2. The Level 2 provider stated that it had not been in control of the ransomware and denied any connection to the criminal activity. However, in its post adjournment correspondence it accepted that the RMIT had been led to the Service via an affiliate marketer with which it was contracted.

   The Level 2 provider confirmed that its affiliate marketing partners are subject to strict conditions and procedures to prevent misleading practices. It provided a detailed summary of the prohibited practices.

3. The Tribunal considered the evidence and submissions before it. In particular, the Tribunal noted the admissions made by the Level 2 provider in relation to the Seller ID of the publisher which led the RMIT into the Service and that it suspected that 69 consumers had been led to subscribe to the Service as a result of the ransomware. 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. As set out in the Background, the Tribunal noted that there was a nexus between the ransomware publisher and the Level 2 provider and therefore the Level 2 provider was responsible for the publisher's promotions for its Service. 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 Avoidance of harm (fear, anxiety, distress or offence)
"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, "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 the extensive submissions set out in response to the breach of rule 2.3.1 of the Code above.

   In addition and specifically in relation to the breach of rule 2.5.5 of the Code the Level 2 provider stated in its written submissions that it did not believe that it could be held responsible for a sense of fear, anxiety, distress or offence as a result of malware that it was not aware or in control of. The Level 2 provider stated that the Service was not designed to create a sense of fear, anxiety, distress and/ or offence and this would be contrary to the Level 2 provider's ethos. However it did accept that fear, anxiety, distress or offence could have been caused by the malware and states that the matter would be more properly dealt with by police.

3. The Tribunal considered the evidence and submissions before it. In particular, the Tribunal noted the admissions made by the Level 2 provider in relation to the Seller ID of the publisher which led the RMIT into the Service and that it suspected that 69 consumers had been led to subscribe to the Service as a result of the ransomware. 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. As set out in the Background, the Tribunal noted that there was a nexus between the ransomware publisher and the Level 2 provider and therefore the Level 2 provider was responsible for the publisher's promotions for its Service. 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
Paragraph 3.4.12(a)
"Level 2 providers must provide to PhonepayPlus relevant details (including any relevant access or other codes) to identify services to consumers and must provide the identity of any Level 1 providers concerned with the provision of the service."

1. The Executive submitted that the Level 2 provider acted in breach of paragraph 3.4.12(a) of the Code as it failed to register the Service as required by the Code.

The Level 2 provider stated that the Service was live for testing from 19 June 2013 and began operation in full on 25 June 2013. The Service was not registered with PhonepayPlus until 1 July 2013.

The Executive accordingly submitted that, for the reason outlined above, the Level 2 provider had operated a Service prior to registering it as required by the Code and in breach of paragraph 3.4.12(a) of the Code.

2. The Level 2 provider accepted that it had operated the Service for a short period of time prior to registration as a result of an oversight. It added that it was not a deliberate attempt to avoid or evade regulation and that it had experienced difficulties with registration and had sought help from the Registration helpdesk.

   During informal representations, the Level 2 provider stated that as a result of human error it thought that the Service had been registered by the Level 1 provider. However, the error quickly came to light without prompt from PhonepayPlus and was quickly rectified in a matter of days.

3. The Tribunal considered the evidence, including the Level 2 provider's admissions. The Tribunal found that the Level 2 provider had failed to register the Service as required by paragraph 3.4.12(a) of the Code prior to the Service becoming operational. The Tribunal noted that the requirement to register a service is an important obligation as non-registration results in consumers not being able to ascertain the details of a service on the Number Checker. Accordingly, the Tribunal upheld a breach of paragraph 3.4.12(a) 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 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 2.14 Promotions and promotional material

   "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 Promotions and promotional material

"There are a number of instances when the combination of colours used in promotional material reduces the clarity of information and the ease with which it 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 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".

Complaint data

The Executive received one complaint on 10 July 2013. The complainant expressed confusion regarding the reason for the charges that appeared on his/her mobile phone bill.

"Stupidly I gave them my mobile number and texted back READY, and then received more messages saying I was subscribing to Brickoffers for £1.50 per SMS! I texted STOP to stop subscription but have just received another text and charged £1.50 again."

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:

- Service pricing;
- how to leave the Service;
- the nature of the subscription Service;
- the dates for the quiz competition which scans across six months;
- there is only one prize on offer;
- a link to the full game terms and conditions;
- 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 terms and conditions were presented in a very small font and required close examination.
b. the terms and conditions are presented in a light blue colour on a dark blue background. The colour combination reduces the clarity of the information and the ease with which it can be seen.

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 denied the breach and stated that it had submitted its Service webpages to its third party advisor for compliance advice and therefore did not believe there was a problem. Further, its other services had a similar design and they are not subject to a PhonepayPlus investigation.

The Level 2 provider stated that consumers were clearly shown all relevant information before purchase and are given an opportunity to complain if they were dissatisfied. The Level 2 provider stated it did not believe consumers were confused as it had not received any complaints about the key terms and conditions.

During informal representations, the consultant acting on the Level 2 provider's behalf stated that he saw the original promotions and considered them to be compliant with the Code. It was strongly refuted that the text was not legible. The consultant stated that he did not know whether the content of the pages viewed by the Executive was the same, especially as the pages he had viewed had a UK customer service number (unlike the pages viewed by the Executive).

3. The Tribunal considered the evidence. The Tribunal considered the promotional screenshots provided by both the Executive and the Level 2 provider (**Appendix F**). The Tribunal took in to consideration that the text appeared clearer on a device than on a photocopied screenshot. However, the Tribunal considered that key terms and conditions material to consumers' decision to purchase were not presented in a manner that was clearly legible. This was as a result of terms being presented in a very small light blue font on a dark blue background. Accordingly, the Tribunal upheld the breach of rule 2.2.2.

   Separate from the breach of rule 2.2.2, the Tribunal commented that it had noted that there was no pricing in the text message containing the means of access to the Service. As a result, it was likely that some consumers may have entered the Service without realising that they would incur charges. Although this did not form part of the breach of rule 2.2.2 (as raised by the Executive), the Tribunal hoped that the Level 2 provider would seek compliance advice on a voluntary basis to ensure that consumers are fully aware of all key terms, most importantly the cost of the Service, prior to incurring any charges. Further, pricing information should be presented in a clear manner, this includes stating the full cost of the Service in a transparent manner.

Decision: UPHELD

SANCTIONS

Initial Overall Assessment

The Tribunal's initial assessment of the breach 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.

Paragraph 3.4.12(a) – Registration of service

The initial assessment of paragraph 3.4.12(a) of the Code was **significant**. In determining the initial assessment for this breach of the Code the Tribunal applied the following criteria:

- The non-registration was for a short period of time.
- The breach was remedied without prompt from PhonepayPlus.
- Registration of services is an important regulatory requirement.

Rule 2.2.2- Written information material 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 criteria:

- The nature of the breach is likely to have caused or potentially caused a drop in consumer confidence in premium rate services.

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 two aggravating factors:

- 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.

The Tribunal noted that the Level 2 provider stated that it suspected that 69 consumers had entered the Service via the non-complaint ransomware route. The Tribunal commented that the number of subscriptions and therefore potential and actual consumer harm was far higher than in the other ransomware affiliate marketing cases.

In determining the final overall assessment for the case, the Tribunal took into account the following three 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 its affiliate network partners that included specific prohibited practices ("Affiliate Marketing Guideline Set").
  - Proactive and extensive testing of affiliate marketing promotions prior to launch.
  - Independent assessment of services for regulatory compliance.
- On being notified of the ransomware affiliate marketing, the Level 2 provider stated that it had:
  - Notified the police.
  - Blacklisted the relevant affiliate network.
  - Implemented enhanced third party monitoring in order to increase control and insight into the online landscape.
  - Temporarily stopped billing all consumers.
- The Level 2 provider stated that it had unsubscribed and offered refunds to all consumers who were likely to have entered the Service via the ransomware route.

The Tribunal rejected the Level 2 provider's submission that the breaches were caused or contributed to by circumstances beyond the reasonable control of the Level 2 provider. The Tribunal noted that following the adjournment the Level 2 provider had taken some time to provide a response to the Executive's questions due to key personnel being on annual leave. The Tribunal commented that where a provider is aware it is under investigation it should ensure that a suitable member of staff is able to respond to information requests in a timely manner.

In addition, the Tribunal noted the following when assessing the overall seriousness of the case:

- The Level 2 provider had not provided any evidence of third party monitoring.
- 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.
- 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 number of leads generated from the ransomware promotion. The Level 2 provider's revenue in relation with this service was in the range of Band 5 (£5,000 - £50,000), which was generated over a very short time period.

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 actual and potential consumer harm had been limited 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 this 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:

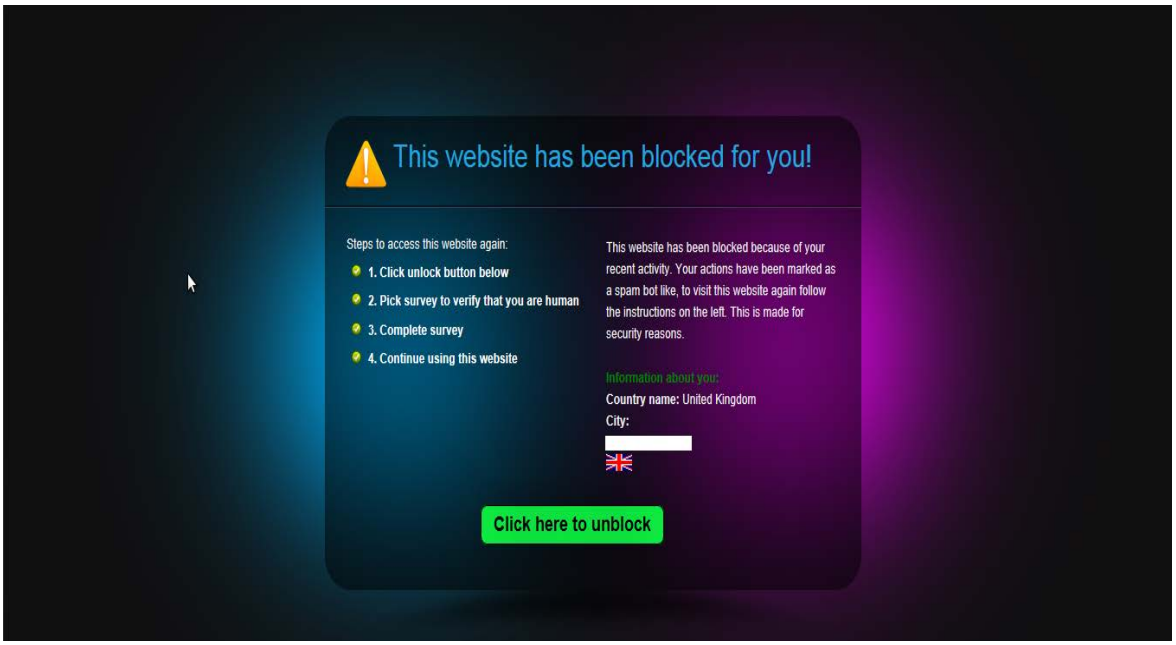
- a formal reprimand;

- 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;
- a fine of £27,000; 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.

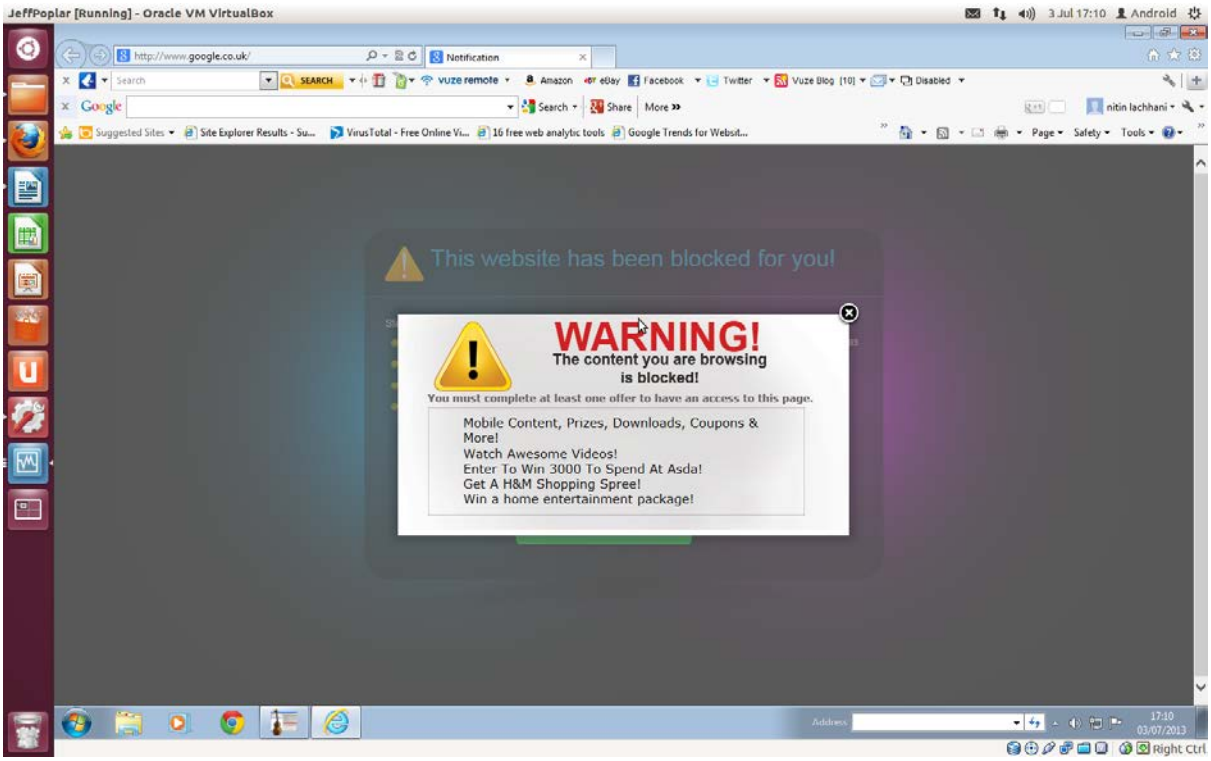
Appendices

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 promotion for the Service on the Funloadia URL:

Appendix E: Further screenshot of a promotion for the Service on the Funloadia URL:

Appendix F: Screenshot of a service landing page provided by the Level 2 provider: