Tribunal Sitting Number 131 / Case 2

Case Reference: 28778

Level 2 provider	R&D Media Europe B.V.
Type of Service	Competition - non-scratchcard
Level 1 provider	Netsize Internet Payment Exchange AB
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, R&D Media Europe B.V. operated an online subscription competition quiz service using the brand names "Zemgo Quiz" and "Zemgo Prizes" (the **"Service"**). The Service operated using Payforit (**"PFI"**) at a cost of £4.50 per weekand was promoted via affiliate marketing. The Level 1 provider for the Service was Netsize Internet Payment Exchange AB.

The Service offered consumers the opportunity to participate in quiz competitions. Consumers were sent a message containing a link to a quiz consisting of ten questions. Each correct answer resulted in a separate entry into a prize draw to win prizes such as an iPhone 5. The winner was selected at the end of the competition period (which ran from 8 February 2013 to 1 June 2013).

The Service operated from 11 February 2013 to 1 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 24 June 2013 and prior to uncovering the ransomware promotions for the Service, the RMIT visited the website "wifihackpassword.com" (**Appendix A**), which offered users a file that purported to enable them to hack into locked wireless networks. The RMIT attempted to download the file (**Appendices B and C**). The monitoring session concluded with the RMIT's Internet Explorer browser being blocked.

The RMIT conducted an additional monitoring session on 25 June 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. The browser displayed a webpage that contained the warning that the website had been blocked and it stated (**Appendix B**).

> "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."

The RMIT clicked on the "Click here to unblock" 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."

Upon clicking on the first offer, to win an iPhone 5, the RMIT was directed to the Service landing page (**Appendix D**) and followed the instructions to complete a multiple choice question (**Appendix E**). The RMIT was taken to a PFI screen which required the RMIT to enter a MSISDN. The RMIT monitoring phone received a free message containing a PIN code. The RMIT entered the PIN on to the PFI page and clicked on "Subscribe Now". The RMIT monitoring phone immediately received a subscription confirmation message and another text message giving the user the opportunity to win a £500 IKEA voucher by following a hyperlink.

On the RMIT computer screen a warning notification appeared, advising that content was blocked and a "survey" had to be completed to gain access to the page (**Appendix C**). At the bottom of the page the RMIT was notified in a pop-up that the download was complete and was given the option of opening or saving the download. The RMIT clicked on "Open" and a notepad screen appeared, containing a password. It is of note that throughout the monitoring session there was never an opportunity to enter or use the password. The RMIT moved away from the tab containing the notepad screen and back to the Service webpage, which contained a quiz with a series of ten questions. The RMIT did not complete the questions and instead closed all tabs/windows. The RMIT attempted to open Internet Explorer and gain access to Google but was again presented with the page informing the RMIT that the website was blocked (**Appendix B**).

The RMIT noted from previous monitoring experiences 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 service.

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

The Investigation

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

On 28 June 2013, the Executive notified the findings of its preliminary investigation to a member of the Code Compliance Panel and obtained authorisation to invoke the Emergency procedure in

relation to the Service pursuant to paragraph 4.5.2 of the Code. The outcome and a direction to suspend the Service was communicated to the Level 2 provider on 1 July 2013. The Level 1 provider was directed to withhold revenue on 1 July 2013. On 2 July 2013, both the Level 1 and 2 providers confirmed that the Service had been suspended.

On 2 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 29 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 30 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 5 August 2013.

The Executive sent a breach letter to the Level 2 Provider on 10 July 2013 and an addendum breach letter on 19 July 2013. Within the breach letter the Executive raised the following breaches of the Code:

2.3.1 - Fair and equitable treatment

2.3.2 - Misleading

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

2.2.2 - Written information material to the decision to purchase

The Level 2 provider responded on 26 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.

Jurisdiction

The Tribunal noted that the Level 2 provider had reported the ransomware to the Police on 23 July 2013 and had asserted that the matters raised by PhonepayPlus were criminal in nature and therefore it was not appropriate for them to be dealt with by PhonepayPlus. The Tribunal noted that PhonepayPlus had contacted the police and was in the process of providing 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

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 attempt 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 attempt 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 was responsible for a breach of rule 2.3.1 of the Code.

The Level 2 provider asserted the Service was not the source of the malware that automatically blocked users' internet browser functionality. Instead, the source of the malware was the website wifihackpassword.com, which it asserted was unsafe by its nature and which captured the Service without the slightest involvement by it. It stated that it did not regard the source of the malware as "marketing" or "promotion" and that it considered it to be an illegal practice as it is, both legally and factually, a form of computer crime or cybercrime in its purest sense. This malware harmed the integrity of (the promotion for) the Service and the PFI scheme.

The Level 2 provider stated that it considers affiliate marketing to be a process whereby a Level 2 provider provides financial consideration to one or more persons or entities in exchange for their agreement to offer content provider's products and/or services to consumers. The person, persons or entity behind this, which introduced the malware had in its opinion committed a criminal act. It submitted that it, or any Level 2 provider, should not and could not be held responsible for an illegal deed of a stand-alone source which is unrelated, but appears to be related because of illegal access to the Service. It added it could not have avoided involvement with the ransomware as its security measures were not immune from computer crime or cybercrime practices.

The Level 2 provider submitted that in order to investigate the matter more thoroughly it needed additional information regarding the RMIT's monitoring of the ransomware activity. It added that it was an, "absolute necessity to view and have insight in the (hidden) components of software and (super) cookies which have been implemented on the device of the RMIT". The Level 2 provider noted that there was a discrepancy in the date shown of the RMIT's monitoring screenshots and the date the monitoring took place on. It asserted that:

> "A probable cause for the date is that the RMIT has monitored our service prior to 25 June 2013 and visited our URL <http://uk.zemgo.com/Production/56?affn=Test>. Downloading the virus or other malware from the unsafe source appears to have copied the information which was prior to 25 June 2013 stored on the device of RMIT. This undoubtedly also has disturbed the time based script of our service and maybe more important a credible performance of the RMIT monitoring."

Furthermore, the Level 2 provider asserted that as the acts in question, appeared to be of a criminal nature, it considered it to be more suitable and appropriate for the police Cyber E-crime unit or the Action Fraud Unit to be the agency that investigates these practices. It stated that it had reported the ransomware to the police itself on 23rd July 2013.

The Level 2 provider added that it had the following questions:

1. Why would any consumer want to visit a website which appears to be dedicated towards conducting further illegal activities (hacking Wi-Fi passwords)?
2. Has the monitoring procedure been tested to ensure the processes are transparent, participative and accountable?
3. What was the benchmark and the criteria for assessment, apart from the PhonepayPlus Code?
4. Were independent reviewers appointed, knowledgeable in both advertising self-regulation and consumer protection issues, and more specifically in the area of cybercrime, for reasons of impartiality and due process?
5. Have appropriate criteria been set up, to check RMIT responses are made correctly by accessing the service online and (re-)viewing responses and results at random?

During informal representations, the Level 2 provider submitted that the breaches should not be upheld. This was on the grounds that:

1. There had been no consumer harm. PhonepayPlus was the only subscriber through the ransomware affiliate marketing promotions.
2. The ransomware promotion was so serious that it should have been reported to (and dealt with by) the police.
3. In future, the Level 2 provider would not use affiliate marketing.

The Level 2 provider thanked the Tribunal for the opportunity to clarify its written submissions, It stated that it was founded in 2001 and was currently active in 21 countries. Its main offices are in the Netherlands and Malaysia. It stated that its focus was to directly liaise and co-operate with operators and regulators to ensure that it correctly interprets regulations and obtains direct feedback. It asserted that in 2011 PhonepayPlus' focus was on co-operation and self-regulation. It claimed that PhonepayPlus had seemingly moved away from the co-operation model and now had a more direct "police" role.

The Level 2 provider stated that a central part of its services was the use of PFI. It claimed that PhonepayPlus had highlighted its preference for PFI in the past in order to ensure that consumers are well informed prior to making a purchase. It asserted PFI is Network-controlled and a trusted payment mechanism.

The Level provider stated that the focus had shifted from its landing pages to the pre-landing pages. It asserted that the pre-landing pages are hosted by affiliate networks and publishers and therefore out of the scope of its services. It said it is also difficult to monitor pre-landing pages. It stated that, since early 2012, it has had a thorough monitoring strategy, which includes:

i. Due diligence on affiliate networks. This includes a credit check, checking the background of directors with PhonepayPlus and Companies House and obtaining references.
ii. Agreements with online publishers.
iii. Specific prohibited practices.
iv. Pre-approval of all marketing and banners etc.
v. Independent monitoring by a set of random consumers.
vi. Independent assessment of services for regulatory compliance.
vii. Blacklisting of non-compliant affiliate marketers and publishers. This included notifying competitors.
viii. Use of an online automated auditing tool.
ix. Use of Cake (an online monitoring tool) since quarter two of 2012, which gives insight and control of affiliate marketing partners. It shows spikes and response ratios. It also gives details of the usage of URLs (i.e. what campaigns are run and where they are

placed). The Level 2 provider showed the Tribunal screenshots of Cake reports, which gave an overview of different affiliate marketers in real time and showed that it was possible to "drill down" on a specific banner/ pre-landing page.

x. A compliance team containing five employees, who actively search the internet and visit pre-landing pages.
xi. In-house third party monitoring by approximately 15-20 students.
xii. Liaison with the consumer services department, which provides weekly updates and feeds regarding the volume and nature of complaints. The consumer services department also incentivises consumers to communicate how they come across the Level 2 provider's services and provide screenshots.
xiii. Monitoring forums and blogs using specialist programmes.

In relation to the ransomware promotion, the Level 2 provider emphasised that it had received no complaints and therefore could not re-create the consumer journey. It stated that the only number affected belonged to the RMIT. It accepted that these facts did not make the situation "all good". Despite its due diligence and monitoring, the online landscape was too big and complicated to get 100% control and that the ransomware activities were illegal. It stated that the hacking website was, "dubious at best," and that it felt that it could not reasonably be held responsible. This was especially true given the aggressive nature of the affiliate marketing. It added that it had decided to stop using affiliate marketing in the UK and focus on own media buy to buy space and generate traffic. But stated that this would take time to set up in-house. It stated that it was limited to how much of a particular consumer's journey it could see.

The Level 2 provider asserted that the ransomware was a criminal act and that it should be dealt with more appropriately by the police cybercrime unit. It had reported the incident to the police on 23 July. It had not been aware of the practice and would never have consented. It controlled, monitored and audited promotions for the Service, but this instance was beyond its control. It added that the definition of the responsibilities of Level 2 providers in the Code (paragraph 5.3.8) could not be interpreted to impose responsibility for the malware on Level 2 providers. If this was within the definition, it submitted that the definition should be changed.

Further, the Level 2 provider submitted that the ransomware promotions did not actually lead to the Service landing pages. It argued that "cookie dropping" had occurred from a previous monitoring session, which had resulted in the RMIT being led to the Service. The Level 2 provider asserted that this was evidenced by the screenshots of the RMIT monitoring displaying the date Sunday 2 June 2013, when the monitoring occurred on 25 June 2013. Later during informal representations, it transpired that the Level 2 provider's own screenshots of its in-house monitoring of the Service also displayed the date of 2 June 2013. On being questioned, the Level 2 provider stated that it did not conduct monitoring on Sundays and did not have an explanation as to why its screenshots of its own monitoring displayed the date of 2 June 2013 also.

The Level 2 provider stated that the only change it could make would be to ensure that its customer service department obtains more information regarding the method of entry.

The Level 2 provider accepted that the affiliate marketers or publishers responsible for the ransomware promotions had financial motives and that there was a potentially a financial nexus between them and itself (albeit remote). However, the parties were untraceable and outside its reasonable control. It stated that it did not think that the incident was "sabotage".

The Level 2 provider added that it was disappointed that PhonepayPlus had not notified it of the ransomware promotions earlier. It added that a notice to industry would have been effective and

the affiliate network could have been blacklisted. It added that, in its view, affiliate marketers should be obliged to register with PhonepayPlus and be regulated.

3. The Tribunal considered the evidence and submissions before it. The Tribunal did not accept the Level 2 provider's arguments in relation to "cookie dropping". It commented that the evidence offered in support of this submission (in relation to the wrong date being displayed on the RMIT's monitoring screenshots) appeared to indicate, on the balance of probabilities, a technical issue with the Service landing pages and not contamination of the RMIT's computer. The Tribunal commented that Level 2 providers are responsible for the operation of their services which includes the promotion of a service. Therefore, where a Level 2 provider chooses to engage in affiliate marketing, it accepts the risk that any affiliate marketing outside its direct control may lead to non-compliance for which it is responsible. Consequently, and for the reasons given by the Executive, the Tribunal concluded that consumers had not been treated fairly and equitably as a result of the malware affiliate marketing promotion in breach of rule 2.3.1 of the Code. Accordingly, the Tribunal upheld a breach of rule 2.3.1 of the Code.

Decision: UPHELD

ALLEGED BREACH 2

Rule 2.3.2

Premium rate services must not mislead or be likely to mislead in any way.

1. The Executive submitted that the Level 2 provider had acted in breach of rule 2.3.2 of the Code as users were likely to have been misled into using the subscription Service and thereby incurred premium rate charges.

   The Executive 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 Service operated using the PFI scheme, which was designed to deliver a secure charge to mobile payment flows. However, the Executive noted that the PFI scheme does not guarantee that all aspects of the Service are fully compliant with the Code as it is not capable of controlling the promotion of a service.

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

   Guidance

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

   Paragraph 3.2
   "PhonepayPlus expects that all promotions must be prepared with a due sense of responsibility to consumers, and promotions should not make any factual claims that cannot

be supported with evidence, if later requested by PhonepayPlus to do so."

Paragraph 3.11
"3.11 No promotion, with particular emphasis on SMS- or MMS-based promotion, should imply that the consumer will be making a one-off purchase, when they will, in fact, be entered into a subscription, or mislead the consumer as to the service they are being invited to purchase."

Paragraph 3.12
"An example of this would be a service that advertised itself as an 'IQ test' or 'love match', where the consumer was then invited to text or click to obtain more in-depth results, only to find that these results carry a further charge, or enter the consumer into an unwanted subscription."

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

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

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

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

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

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

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

Spotify Codes

On 23 April 2013, the RMIT conducted an additional monitoring of the Service and discovered that it was promoted by affiliate marketers. The RMIT searched on Google for free code

generators that purport to gain access to the Spotify service for free. Spotify is an online music streaming and download service; users pay a minimum of £4.99 per month to access the website and its content. The RMIT selected one particular offer and was taken to a number of screens which appeared to indicate that a Spotify code file could be downloaded. The RMIT was eventually presented with a message that stated:

> "Success, You found a Spotify Premium Code, Click OK to get your code from a secured server"

After clicking "OK" the RMIT was asked to complete a survey in order to unlock the download. The RMIT selected an option that stated, "Chance to win an IPhone 5! Mobile rates apply," and the RMIT was subsequently directed to the "Zemgo Quiz" Service landing page. The RMIT subscribed to the Service and attempted to download the Spotify codes but was unsuccessful. The Executive asserted that the codes were, in fact, fake and the affiliate marketing campaign was a misleading inducement to encourage consumers to sign up to a premium rate service.

The Executive further asserted that consumers would have been misled by the Spotify codes campaign as it was highly likely that a consumer would have been led to believe that, by entering into the premium rate service, s/he would eventually obtain the codes.

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

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

Mark Zuckerberg Facebook credits

On 21 May 2013 the RMIT conducted additional monitoring of the Service by searching on a monitoring phone for "free Facebook credits" using Twitter. The RMIT discovered a series of tweets that had allegedly been written by the creator of Facebook, Mark Zuckerberg. The RMIT selected one tweet and was taken to a new page which purported to be Mark Zuckerberg's Twitter account. The RMIT selected a highlighted link and was immediately redirected to a list of "offers", whereupon the RMIT selected one which stated:

> "Chance to win an iPhone 5! Mobile rates apply"

The RMIT was directed to the Service landing page. On this occasion, the RMIT did not subscribe to the Service but the Executive submitted that it was highly unlikely that the Mark Zuckerberg credits existed as an offer to obtain unlimited free Facebook credits would have been unrealistic and commercially unviable. The Executive further submitted that, even if the offer for free Facebook credits was genuine, the promotion was likely to mislead consumers into signing up to a premium rate service that had no connection to Facebook credits.

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 the content of its response to the alleged breach of rule 2.3.1 of the Code.

In addition it stated that the fake Spotify codes and fake Facebook credits, "are seemingly not as

criminal as the malware example", but that realistically, it could not be held responsible, as the examples of the fake Spotify codes and the fake Facebook credits were "malware orientated", which infected the correct access to and distribution of the Service.

Further, the Level 2 provider stated that the main reason for it abandoning all its previous payment flows and implementing the PFI payment method was to ensure that consumers were made aware of both the service they are about to enter and the costs of the service. It asserted that PhonepayPlus had outlined its preference for the implementation of PFI. Therefore, regardless of whatever other advertisements the consumer is presented with, the pre-landing page, the actual landing page and the PFI flow ensure the consumer is properly made aware of the product he or she is purchasing. It submitted that consumers who assert that they were not aware of the costs of a Service were wrong and that dissatisfaction came from disappointment in the quality of the quiz service. Although this argument was not within the scope of this investigation, it stated that it will abandon the current quiz service and launch other content services that will be more satisfactory for consumers.

The Level 2 provider commented that more recently, new types of online advertisements have flooded the market. It added that although the flows presented might differ from each other they all share the same nature: they are illegal, they are not part of regular affiliate marketing and are not in the scope of what content providers can reasonably be held responsible for. Whether it is malware that blocks the internet browser, a fake copy of "Whatsapp" or a person presenting himself as Mark Zuckerberg, these, the Level 2 provider said, were all scams to that extent it should be investigated by the police rather than PhonepayPlus. These were, it continued all illegal activities which break "regular" laws, and are out of the scope of the PhonepayPlus Code. It added that it was not aware of the scams taking place and would obviously never give its consent to these practices had it been aware.

In summary, the Level 2 provider stated that it had taken or intended to take the following action:

i. Terminated the subscriptions of all affected end users.
ii. Offered a full refund for users complaints in relation to the "scams".
iii. "Close[d] down" all affiliate marketing for the Service.
iv. Creating new content services and setting up direct media buying.
v. Implement advanced monitoring tools that can track the entire flow of online clicks.

3. The Tribunal considered all the evidence and submissions before it. The Tribunal commented that Level 2 providers are responsible for the operation of their services, which includes the promotion of a service. Therefore, where a Level 2 provider chooses to engage in affiliate marketing, it accepts the risk that any affiliate marketing outside its direct control may lead to non-compliance for which it is responsible. Consequently, and for the reasons 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 Executive's reason 1). The Tribunal concluded that there had been a breach of rule 2.3.2 of the Code. The Tribunal also found that consumers were likely to have been misled into the Service as a result of affiliate marketing promotions that purported to offer free Spotify codes (the Executive's reason 2). 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 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 stated that the assertions that entering the Service was a result of the malware, was based on the suggestion that it was aware of the malware. It added that whatever the basis for this assertion, it could not be held reasonably accountable for the creation of an unreasonable sense of fear, anxiety, distress or offence. Further, the Service was not designed to create such a sense of total non-compliance. It asserted that the ransomware was in total contradiction with its ethics, and also harmed the entire mobile sector. It reiterated that the sense of fear, anxiety, distress or offence:

> "[B]elongs within the domain of the law on computer crime and is not be regulated by the PhonepayPlus but is in fact investigated and enforced by the Metropolitan Police. We are still very surprised that PhonepayPlus consider they are responsible and not the Police in investigating these criminal acts. We are actively supporting the Police in their on-going investigation into this issue and a report has been filed with them."

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

Decision: UPHELD

ALLEGED BREACH 4

Rule 2.2.2

All written information which is material to the consumer's decision to purchase a service must be

easily accessible, clearly legible and presented in a way which does not make understanding difficult. Spoken information must be easily audible and discernible

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' and 'Competition and Games with other prizes'.

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

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

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

   Paragraph 1.1 Competitions and Games with other prizes
   "All promotional material should provide clear details as to how the competition operates. Consumers must be made aware, before entering into the service, of any information that is likely to affect their decision to participate. Clear terms and conditions should include, but are not limited to:
   •Information on any restrictions on number of entries or prizes that can be won;
   •The incremental cost and the full cost of participation, where this is known".

   Monitoring

   The Executive relied on the monitoring of the Service carried out by the RMIT and detailed in the "Background" section. The Executive submitted that consumers were not clearly made aware of key terms and conditions at the outset. The Executive submitted the key information was as follows:
   - pricing;
   - the nature of the subscription service;
   - opening and closing dates for the competition;
   - details of how to leave the service;
   - the Level 2 provider's contact details; and

- a route of free entry to the service.

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 E**), because;

a. the key information, save for the first three bullet points above, appeared below the fold on the Service landing pages; and
b. the terms and conditions were presented in a very 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 denied the breach. It submitted that all key information was evident and prominently visible above the fold on all its website pages. It provided a significant number of screenshots in support of its arguments. In all the screenshots, the key information was displayed above the fold (**Appendix F**).

The Level 2 provider added that consumers also received messages which contained key information, such as the cost of the Service, method of exit instructions and the customer service telephone number.

During informal representations, the Level 2 provider stated that all necessary information was communicated to consumers prior to purchase and regardless of the content of pre-landing pages. It added that when viewed on an iPad the key information was not cut off. It added that it did not control the PFI pages. It added that the reason some information was displayed below the fold in monitoring was due to the number of toolbars on the RMIT's computer (three). It stated that it designed its pages on the basis of the most used consumer settings and screen resolutions.

On being questioned, it stated that the large white space between the call to action and the terms and conditions was a result of how the page was designed for mobile devices. It added that pages designed to be displayed on computer devices displayed the key terms above the fold. Further, it asserted that the space was as a result of HTML coding and potentially not something that could be modified.

In summary, it stated that:

1. there were no complaints;
2. the delay in notification of the ransomware promotion by PhonepayPlus was an aggravating factor;
3. a warning to industry would have been "incredibly useful" and would have resulted in more timely checks; and
4. the ransomware was a criminal matter and it was perplexed that PhonepayPlus had not reported the matter to the police.

3. The Tribunal considered the evidence before it and said it was concerned that the important information might not appear above the fold if the user has several toolbars (which it did not consider to be an unlikely scenario). It was also concerned about the large area of white space between the call to action and the terms and conditions, and questioned whether this was really necessary. However, given that the information would have displayed on the screen without having to scroll if the RMIT had not had toolbars installed, and given the lack of complaints from

consumers, the Tribunal decided not to uphold a breach of rule 2.2.2 of the Code. The Tribunal noted that this decision was made on the specific facts of this case and did not bind future Tribunals from making a different determination where toolbars required scrolling to see the full terms and conditions. The Tribunal commented that it hoped that the Level 2 provider would seek compliance advice in relation to the issues raised by the Executive.

Decision: NOT 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.

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:

- 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 Level 2 provider had a relevant breach history in which it had been fined £100,000 for affiliate marketing which breached the Code of Practice

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:
  - Due diligence on affiliate networks.
  - Agreements with online publishers.
  - Specific prohibited practices.
  - Pre-approval of all marketing and banners etc.
  - Independent monitoring by a set of random consumers.
  - Independent assessment of services for regulatory compliance.
  - Blacklisting of non-compliant affiliate marketers and publishers. This included notifying competitors.
  - Use of an online automated auditing tool.
  - Use of Cake (an online monitoring tool) since quarter two of 2012.
  - A compliance team containing five employees, who actively search the internet and visit pre-landing pages.
  - In-house third party monitoring by approximately 15-20 students.
  - Liaison with the consumer services department, which provides weekly and feeds regarding the volume and nature of complaints.
  - Monitoring forums and blogs using specialist programmes.
- On being notified of the ransomware affiliate marketing, the Level 2 provider:
  - Notified the police.
  - Blacklisted the relevant publisher.
  - Implemented enhanced third party monitoring.
  - Made the decision to promote the Service using alternatives to affiliate marketing.

The Tribunal noted that the Level 2 provider asserted that a very limited number of consumers had been affected and that this small number of consumers had been offered a refund.

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

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

The Tribunal noted the Level 2 provider's assertion in relation to the limited number of leads generated from the ransomware promotion. The Level 2 provider's revenue in relation to the Service was in the range of Band 5 (£5,000- £50,000).

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

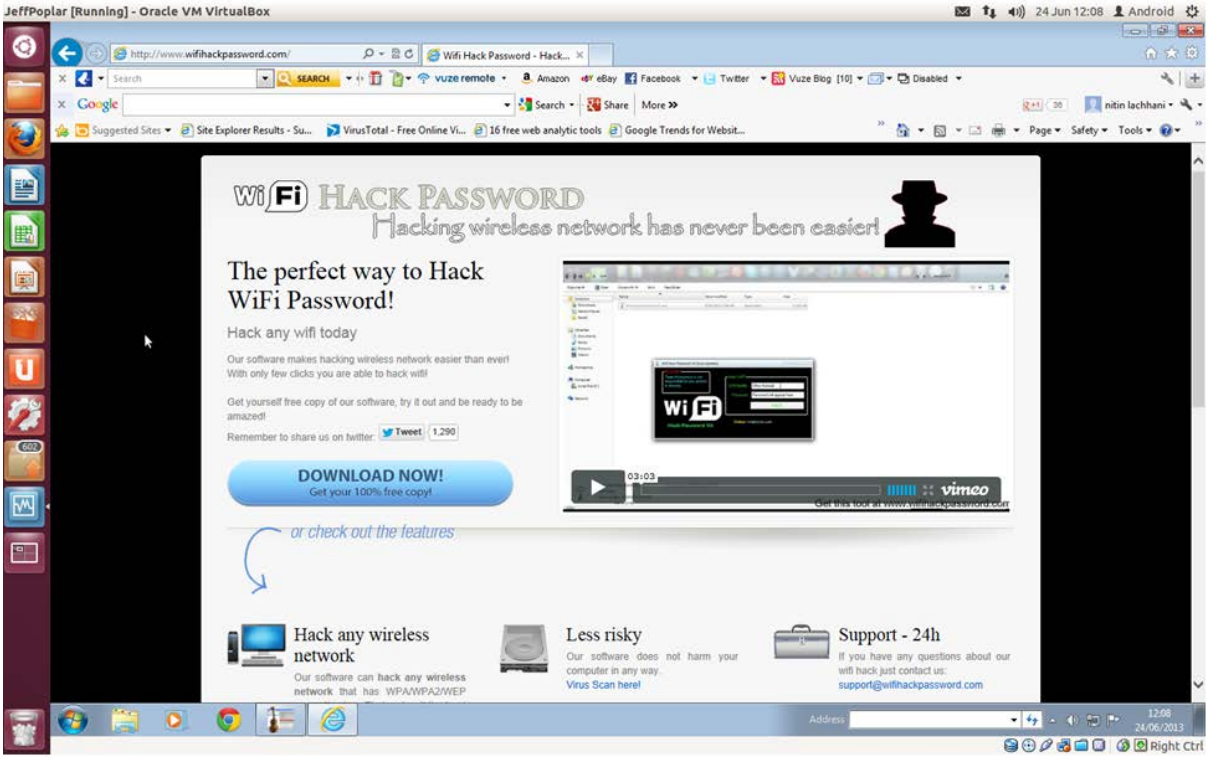
Sanctions Imposed

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

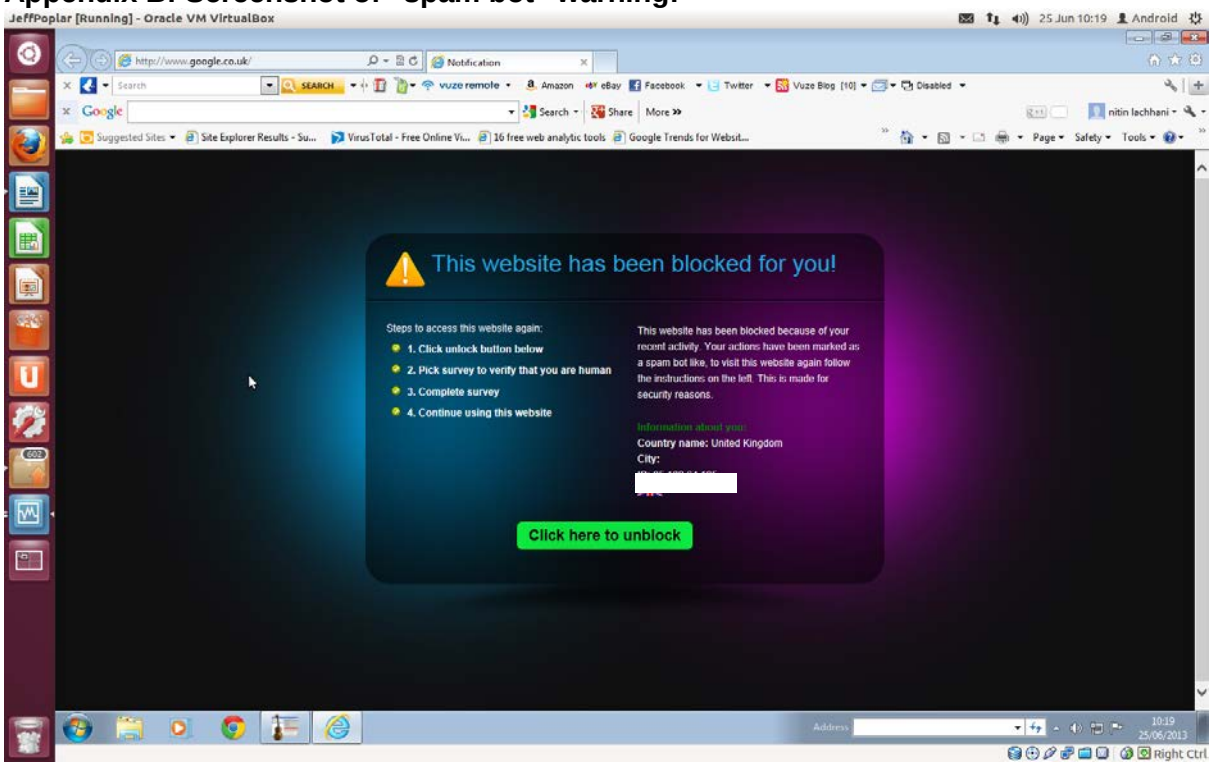
- a formal reprimand;
- a warning that this was the second time the Level 2 provider had been adjudicated against as a result of non-complaint affiliate marketing promotions and that if the Level 2 provider fails to ensure that it has sufficient measures in place to prevent actual or potential consumer harm being caused by affiliate marketing in future it should expect to receive a significant penalty;
- a fine of £40,000 (including a £15,000 uplift which was imposed as a result of the Level 2 provider's relevant breach history); 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

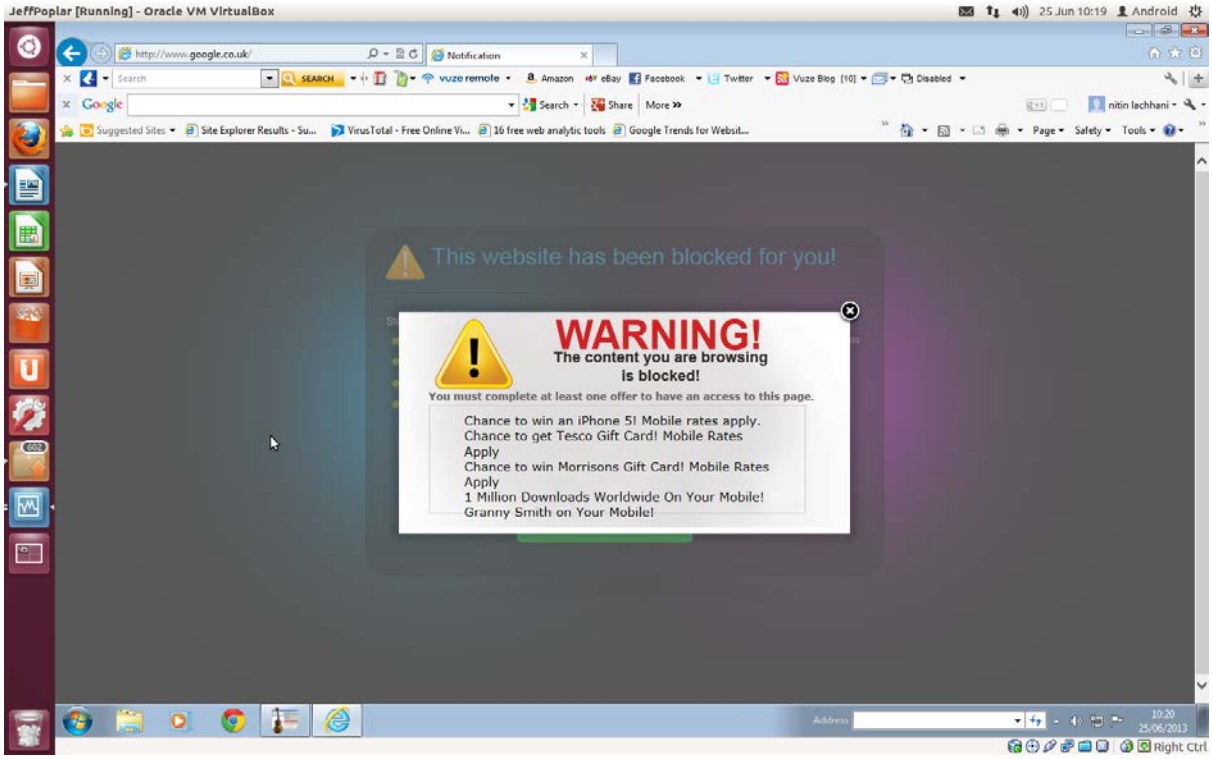
Appendix A: Screenshot of wifihackpassword.com:



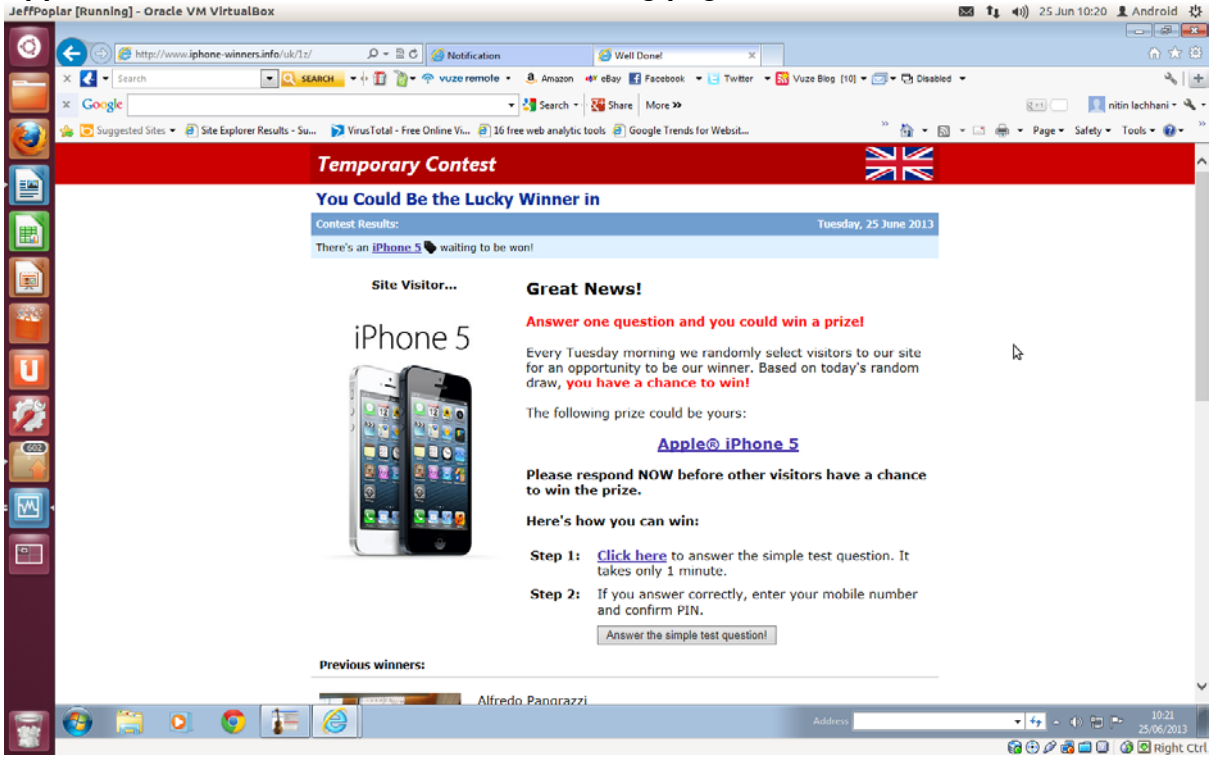
Appendix B: Screenshot of "spam bot" warning:



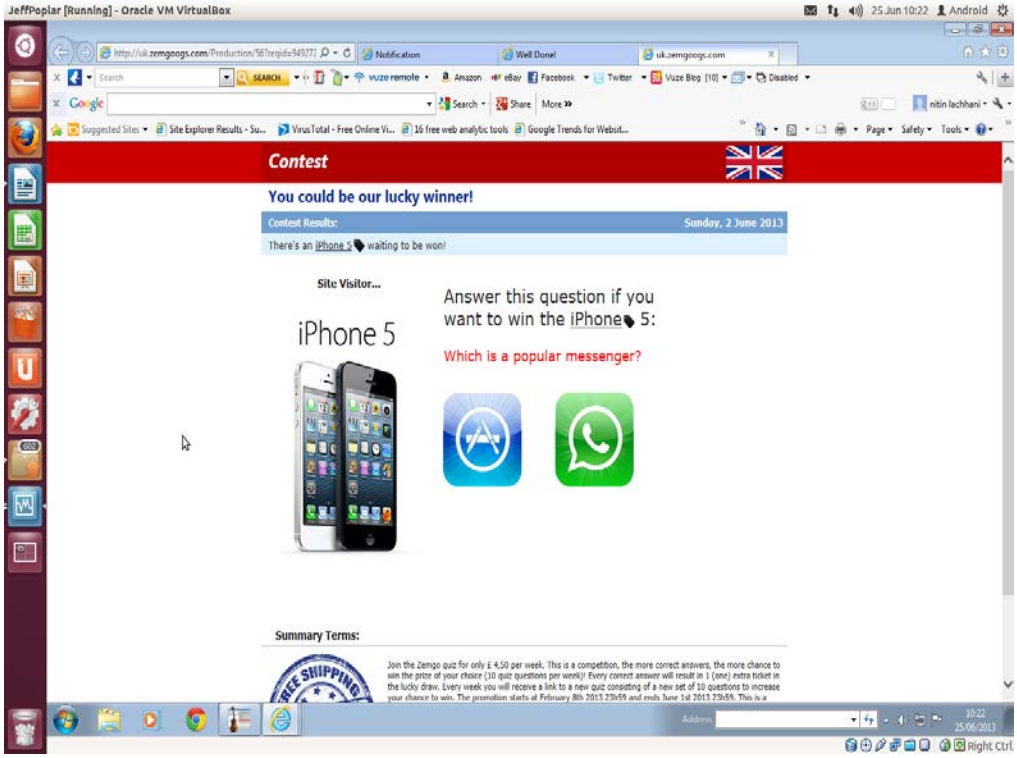
Appendix C: Screenshot of "Warning" webpage:



Appendix D: Screenshot of the Service landing page



Appendix E: Screenshot of the Service webpage containing quiz questions:



Appendix F: Screenshot of a Service landing page submitted by the Level 2 provider: