Code Compliance Panel

Tribunal Decision

Tribunal Sitting Number 130 / Case 1

Case Reference: 28782

Level 2 provider	Jesta Digital GmbH
Type of service	Mobile download
Level 1 provider	Velti DR 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, Jesta Digital GmbH, trading as "Jamster" operated an online subscription content download service using the brand names "Jamster Action Club" and "The Tone Club" (the **"Service"**). The Service operated on the premium rate shortcode 88888 and via Payforit ("**PFI**"), and cost £4.50 per week. The Level 1 provider for the Service was Velti DR Limited.

The Service offered consumers the opportunity to download unlimited mobile content such as ringtones, games and wallpapers. The PFI service operated from 3 June 2013 to 2 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 (the**"RMIT"**). The monitoring revealed that affiliate marketing promotions, which generated consumer traffic to the Service, appeared to utilise a form of malware (ransomware) that stopped consumers' internet browsers from working, resulting in users' being unable to access a large number of popular websites, including Facebook, Ebay, Google. Users were told that they were required to sign up to the Service (and/or other premium rate services) in order to unblock their browsers.

Between 25 June 2013 and 2 July 2013, the Executive received six complaints from consumers, although none specifically concerned the ransomware affiliate marketing.

Monitoring

On 12 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, C and D**). 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 the Google homepage was still blocked. The browser displayed a webpage that contained the warning that the website had been blocked (**Appendix D**). In exactly the same manner as before, the RMIT were directed to complete a "survey" to win products. Upon clicking on a product, the RMIT were directed to the Service landing page (**Appendix E**) and followed the instructions to subscribe to the Service via PFI. The RMIT eventually closed all the browser windows that had been opened during the monitoring session

and opened a new browser window to attempt to access the Google search engine but again a notification tab appeared which stated that the website was blocked (**Appendix D**).

The RMIT noted that during both monitoring sessions, completing the "offers" resulted in users subscribing to a premium rate service but the internet browsers that were blocked by the malware were not unblocked following entry into the subscription Service. It is of note that in order to unblock its internet browser the RMIT had to re-boot its desktop in "safe mode" and eliminate all viruses using its existing security software. The Executive noted that it is likely that 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 one 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 and the Executive directed the Level 2 provider to suspend the Service immediately. The Level 1 provider was directed to withhold revenue on 1 July 2013. On 2 July 2013, the Level 2 provider 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 a notification on its website, stating that the Emergency procedure had been invoked. On 4 July 2013 the Level 2 provider requested a review of the use of the Emergency procedure. The Tribunal declined the application for review, as it was out of time. The Executive sent a breach letter to the Level 2 provider on 10 July 2013. Within the breach letter the Executive raised the following potential 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)
- Rule 2.2.2 – Written information material to the decision to purchase

The Level 2 provider responded on 17 July 2013. On 25 July 2013 the Tribunal reached a decision on the breaches raised by the Executive. The Level 2 provider made informal representations to the Tribunal.

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.

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 a 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 an 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 subscription Service in order to unblock their browsers (**Appendix D**).

   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 is wholly responsible for the content of promotional material used to market the Service was 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 had acted 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 made detailed written and oral submissions. In summary, it accepted that the promotions were examples of aggressive affiliate marketing techniques and did not treat consumers fairly or equitably. However the Level 2 provider asserted that it was not its intention for the Service to be promoted in the manner observed by the Executive. The Level 2 provider accepted that it used affiliate marketers and stated that it was a necessary component of its business (and for any business competing in this arena). However it appreciated that there were risks in using affiliates because, as it saw it, full control of an affiliate was impossible. The structures of affiliate networks were constantly changing, which meant that they were diverse and challenging to control. The promotion in question was from a publisher who had gone ahead without its knowledge or approval.

   The Level 2 provider stated that it had always taken care to ensure its affiliates respect the law. Where non-compliance is detected the Level 2 provider stated that it takes robust action. For example, it had taken action against an affiliate marketer which had induced a consumer to its service with the false promise of an iPad, which was against its policies. The Level 2 provider stressed the efforts it had made to ensure its promotions were compliant namely:

   - conducting its own monitoring of marketing and consumer complaints to recognise any areas of suspicion;
   - imposing restrictions on its affiliate marketers through express terms in their contracts;
   - visibility of standard contracts between affiliate networks and sub-affiliates;
   - pre-approval of promotions; and
   - researching the reputation of the affiliate network before contracting.

   The Level 2 provider noted that it had the most to lose when its Service was promoted through illegal means by a rogue affiliate and raised the following arguments. First, whilst accepting that the promotions did not treat consumers fairly or equitably, it questioned whether the Service had caused any harm to consumers. It argued that it was the Service and its direct advertising which was subject to regulation, not the promotions of sub-affiliate publishers.

   Secondly, the Level 2 provider questioned the level of protection that should be afforded to those who were likely to be affected on the facts of this case. The Level 2 provider noted that the Executive found the ransomware through a website that purported to hack Wi-Fi passwords. Therefore a consumer looking for dubious content may have lost the right to the same level of protection. The Level 2 provider drew the Tribunal's attention to the fact that there was only one real subscription, which demonstrated that not many consumers were affected.

   Lastly, the Level 2 provider made detailed representations on the issue of causation and remoteness, in particular whether the Level 2 provider could be held wholly accountable for the actions of an affiliate marketer.

   The Level 2 provider produced the following documents:

   i. Its service terms and conditions.
   ii. An agreement with the Level 1 provider.
   iii. Its warning letter to affiliate marketers.

During informal representations, the Level 2 provider added that it had operated in the UK market for the last ten years and was extremely surprised by the recent ransomware attack. It stressed that it took this type of "illegal" affiliate marketing very seriously but commented that the market was very fragmented and that affiliate networks operate behind other affiliate networks, "subselling" and "bidding". It added that it was constantly learning about affiliate marketing. It stated that it was a necessity to use affiliate marketing but that it was aware of the risks.

In the future the Level 2 provider stated that it intended to carry out the following additional steps:

- to review and renegotiate its terms and conditions with its affiliate marketers; and
- to raise awareness of affiliate marketing issues amongst industry bodies in the hope that there would be an industry solution to make the affiliate networks understand their responsibility.

The Level 2 provider explained that up until the end of 2012 it contracted with one affiliate network which it trusted and in which it had confidence that its advertising methods were legitimate. It stated that, whilst it was now aware that there was mention of ransomware in blogs at the end of 2012, at the time in question it had such trust in its affiliate that it did not consider that there was a risk in relation to the promotion of its Service. It then contracted with another two affiliate networks and accepted that the risks increased.

In relation to looking at upstream data to ascertain the origins of traffic to the Service, the Level 2 provider asserted that it could only look as far as it was allowed by the affiliate network because it was common practice for the affiliate network to hide the identities of the sub-affiliates to prevent the Level 2 provider contacting them directly.

In summary, the Level 2 provider confirmed that it was disappointed by the situation. It stated that it was not wilfully involved with the ransomware and it planned to continue to look for ways to improve and reduce the risks associated with affiliate marketing.

3. The Tribunal considered the evidence and submissions before it, the Tribunal noted that the Level 2 provider accepted that the affiliate marketing malware promotions were "illegal" and in breach of the Code. The Tribunal commented that Level 2 providers are responsible for the operation of their services, which includes the promotion of a service. Therefore, where a Level 2 provider chooses to engage in affiliate marketing, it accepts the risk that any affiliate marketing outside its direct control may lead to non-compliance for which it is responsible. The Tribunal did not accept the Level 2 provider's submissions on the scope of regulation, causation and remoteness. 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 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 £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 PFI scheme does not guarantee that all aspects of the Service are fully compliant with the Code as it was designed to deliver a consistent payment flow/experience and is not capable of controlling the promotion of a service.

   The Executive noted that the Level 2 provider was 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 Services were promoted via affiliate marketing. The RMIT monitored the Service. The monitoring demonstrated that users were led into the Service via affiliate marketers having 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 file (**Appendix B**). Having clicked "Download" the user received a "WARNING!" notification informing that the required content 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 the Level 2 provider's Service landing pages and whether or not the user interacted with the Service 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, where 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 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 has acted in breach of rule 2.3.2 of the Code as a result of misleading affiliate marketing for the Service.

2. The Level 2 provider acknowledged that the promotions were inherently misleading. However, it stated that the promotion was not authorised or "tolerated".

   The Level 2 provider reiterated the oral and written submissions it had made in response to the alleged breach of rule 2.3.1.

3. The Tribunal considered all the evidence and submissions before it. The Tribunal noted the Level 2 provider accepted that the affiliate marketing malware promotions were misleading, "illegal" and in breach of the Code. The Tribunal commented that Level 2 providers are responsible for the operation of its services, which includes the promotion of a service. . Therefore, where a Level 2 provider chooses to engage in affiliate marketing, it accepts the risk that any affiliate marketing outside its direct control may lead to non-compliance for which it is responsible. Consequently, and for the reasons given by the Executive, the Tribunal concluded that consumers were likely to have been misled as a result of a number of misleading statements contained within the affiliate marketing promotions for the Service, into downloading malware and into believing that entering the Service would "unblock" their internet browsers. The Tribunal concluded that a breach of rule 2.3.2 of the Code had occurred. 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 spambot like, to visit this website again follow the instructions on the left. This is made for security reasons."

Monitoring

The Executive relied on the details of 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 was 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, despite following the instructions to unblock their browser, the browser continued to be compromised. At this point, the user was likely to have had no idea how to rectify the situation and unblock his/her 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 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 or offence.

Additionally, users who understood that their internet browser had been infected with malware would have been likely to have experienced fear, anxiety, distress 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 D)

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 have 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 generally accepted the promotions would cause fear, anxiety, distress and/ or offence but maintained that this had occurred unbeknown to it, as it originated from a rogue affiliate.

   In addition, the Level 2 provider questioned whether the page which carried the "WARNING!" notice would cause fear and anxiety to an "average consumer" as consumers were generally aware of phishing and spoofing attacks.

   The Level 2 provider drew a distinction between the promotion and the Service itself, and made clear the Service did not cause fear and anxiety. It added that:

   > "Users who think that their desktop security might have been compromised may experience some kind of frustration, however due to the fact that their desktop has indeed been infected it seems that their desktop was not properly prepared against malware through the use of anti-virus software."

   The Level 2 provider reiterated its detailed written and oral submissions made in relation to rule 2.3.1 of the Code.

3. The Tribunal considered all the evidence and submissions before it. The Tribunal commented that Level 2 providers are responsible for the operation of their services, which includes the promotion of a service. Therefore, where a Level 2 provider chooses to engage in affiliate marketing, it accepts the risk that any affiliate marketing outside its direct control may lead to non-compliance for which it is responsible. Consequently, and for the 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 discernable.

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 Services 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 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 5.6 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."

Complaints

The Executive noted the content of the following complaints:

"Summary of Complaint: 3 texts a week @ £1.50 per text for the last 10 weeks total = £45 including VAT. Surely this cannot be fair. O2 are aware that this number is my daughters and that she is twelve years old. Surely somebody in customer services should ring to check on this erratic new activity on this number. Jamster also charged when she stopped the download. It does not even say how to get rid of it. I have tried texting STOP and hope this works. Doesn't anyone have to check with the bill payer first?"

"Consumer 13 year old grandson has been receiving unsol[icited] premium rate text messages from 8888.Consumer grandson did admit he downloaded one song but believed this was a one off and doesn't believe he subscribed to a service."

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;
- Details of how to leave the service;
- The Level 2 provider's contact details;
- Age restriction; and
- Link to the terms and conditions.

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

a. the key information appeared below the fold on the Service landing pages;
b. the terms and conditions were presented in very small font and required a close examination; and
c. the terms and conditions are presented in white on a dark beige background which adversely affected the clarity.

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

2. The Level 2 provider accepted that the information contained in the terms and conditions did not meet the requirements of the Code and explained it was an oversight. Upon being made aware of the problem, the Level 2 provider immediately instructed its marketing department to lift the key terms and condition above the fold and to present them in a way that is easily accessible, clearly legible and not difficult to understand.

The Level 2 provider stated that it believed that the landing page in question was compliant, having

relied on the web accessibility guidelines "W3C", but was open to any suggestions from PhonepayPlus and would make any improvements required before the Service commenced operation again.

During informal representations, the Level 2 provider accepted that the information on the landing pages in question did not meet the Code's requirements.

3. The Tribunal considered the evidence, including the Level 2 provider's representations and admissions. The Tribunal found that the position, font size and colour scheme of key terms on the particular landing page in question resulted in the terms that were material to the consumer's decision to purchase not being accessible, clearly legible and presented in a way that was not difficult to understand. Consequently, for the reasons advanced by the Executive, the Tribunal concluded that promotional material on the Service landing pages submitted by the Executive was not complaint with rule 2.2.2 of the Code. Accordingly. The Tribunal upheld a breach of rule 2.2.2 of the Code.

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 the 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 the 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 or offence)

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

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

Rule 2.2.2 – Written 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 the breach of the Code the Tribunal applied the following criteria:

- The Service had promotional material that was designed to not provide consumers with adequate knowledge of the Service and the costs associated with it.
- The breach was isolated to a small number of promotions.

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

Final Overall Assessment

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

- The Level 2 provider failed to follow Guidance on Promotions and promotional material and Competitions and other games with prizes.
- 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 without having any sufficient systems in place to prevent or detect improper practices.

The Level 2 provider had no relevant breach history.

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

- The Level 2 provider stated that it had the following measures in place to identify and mitigate against the risks associated with affiliate marketing:
  - Contracts with the affiliate networks with which it had a direct relationship. The contracts contained a number of restrictions including penalty clauses for non-compliant behaviour.
  - Visibility of standard contracts between the affiliate networks and its sub-affiliates
  - Proactive monitoring conducted on an on-going basis and as a result of:
    - Spikes in traffic
    - Complaints
  - Pre-approval of all marketing flows.
  - Pre-contract research in relation to the affiliate network's reputation

- The Level 2 provider stated it has taken action to ensure the risks of any breaches reoccurring are minimised including:
  - Sending a warning letter to its affiliate networks threatening a financial penalty of 1000 Euros if their promotions are non-complaint and/or involved any illegality.
  - In the future the Level 2 provider plans to review and renegotiate its terms and conditions with its affiliate networks.
  - It intends to enforce contractual requirements that impose restrictions and indemnities on the affiliate networks.
  - Build relationships with industry bodies to raise awareness of the issue of affiliate marketing.

The Tribunal noted that the measures 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 found that the Level 2 provider's relevant revenue in relation with 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 proportion of the Level 2 provider's revenue appeared to be from legitimate sources. 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.**

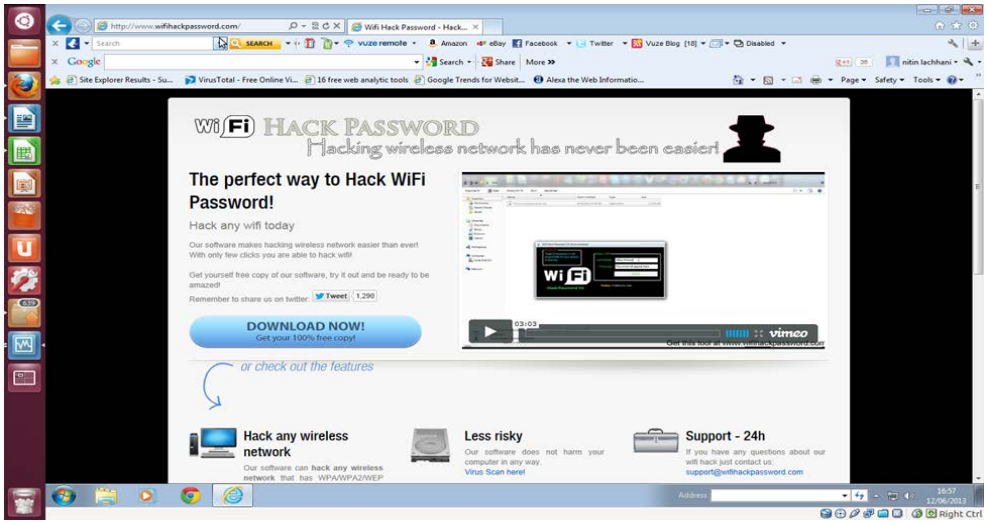
Sanctions Imposed

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

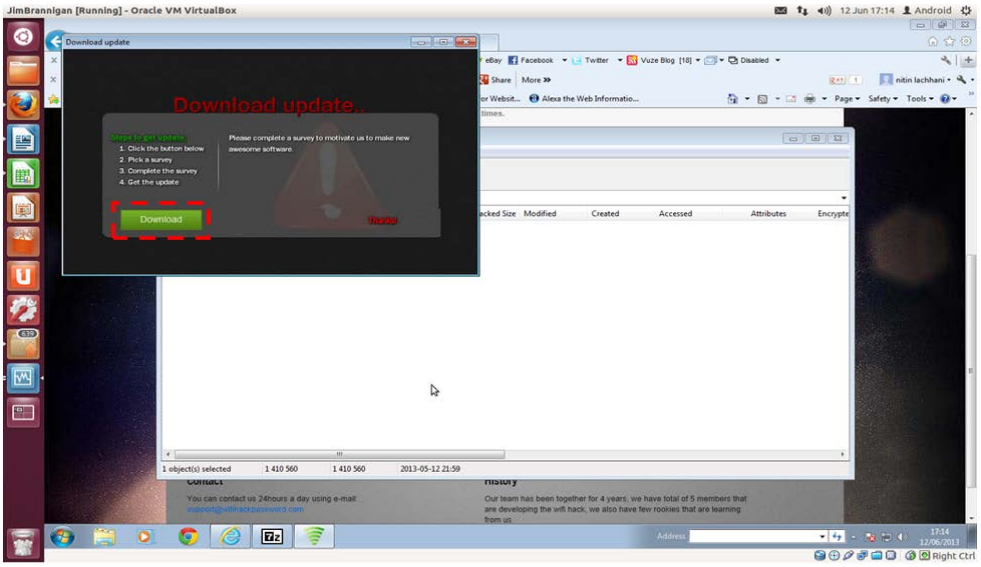
- a formal reprimand
- a warning that if the Level 2 provider fails to ensure that it has sufficient measures in place to prevent actual or potential consumer harm being caused by affiliate marketing in future it should expect to receive a significant penalty for any similar breach.
- a fine of £25,000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

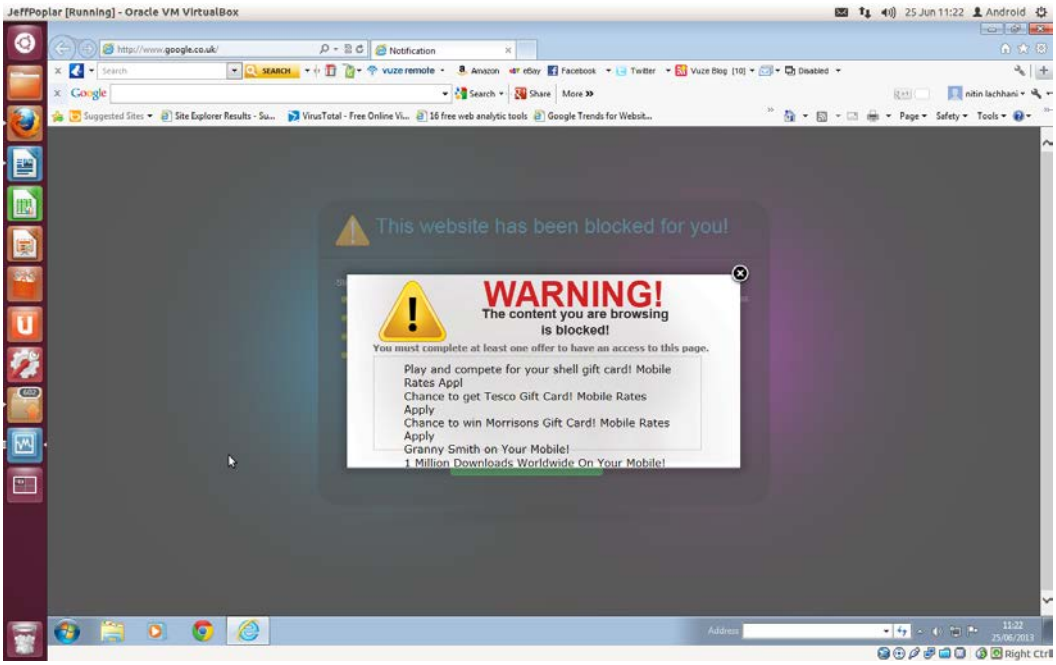
Appendix A: Screenshot of Wifihackpassword.com:



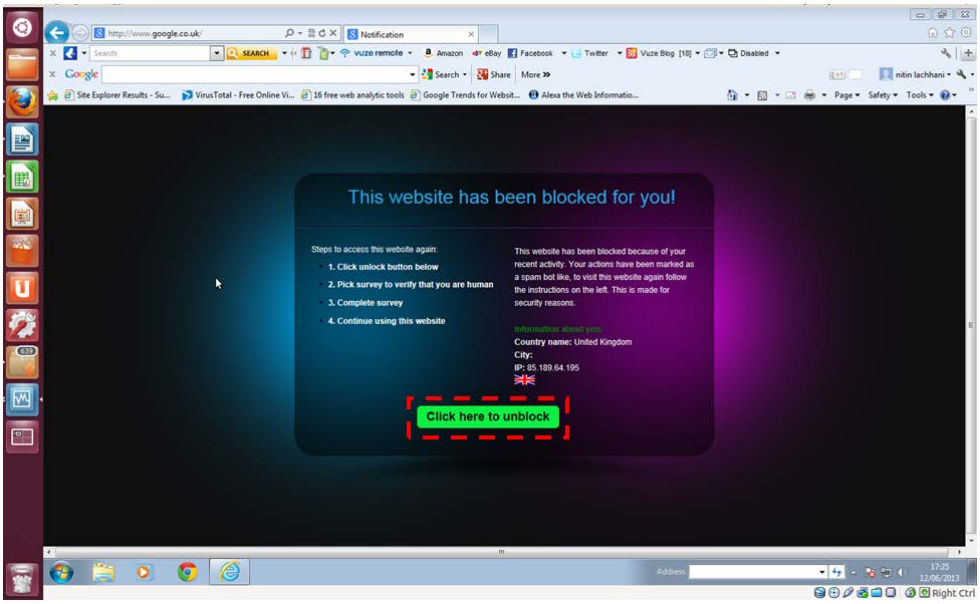
Appendix B: Screenshot including the dialogue box offering an update:



Appendix C: Screenshot of the “Warning” webpage:



Appendix D: Screenshot of “spam bot” warning:



Appendix E: Screenshot of the "Granny Smith on your mobile" Service landing page:

Appendix F: Screenshot of a Service landing page: