Tribunal Sitting Number 130 / Case 5

Case Reference: 28785

Level 2 provider	GICO (Europe) LLP
Type of service	Competition - non-scratchcard
Level 1 provider	MC Mobile Connectivity GmbH and Velti DR Limited
Network operator	All Mobile Networks

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

BACKGROUND

The Level 2 provider, GICO (Europe) LLP, operated an online subscription competition quiz service using the brand name "Triviato" (the "**Service**"). The Service operated on the premium rate shortcode 80876 at a cost £4.50 per week. The Level 1 providers for the Service were MC Mobile Connectivity GmbH and Velti DR Limited.

The Service offered consumers the opportunity to participate in monthly quiz competitions. Consumers were required to answer ten questions. The person who answered the most questions in the fastest time every month won a prize, such as a Shell giftcard.

The Service operated from September 2012 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 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 8 November 2012 and 28 June 2013, the Executive received nine 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 that it could not access the Google homepage as it 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 was directed to complete a "survey" to win products. Upon clicking on the first offer the RMIT was directed to the "Triviato" landing page (**Appendix E**) and

followed the instructions to complete a quiz question, which required the RMIT to enter a MSISDN. The RMIT monitoring phone received a free message to which the RMIT responded with the trigger word contained within the message received. This was immediately followed by a subscription confirmation message. The RMIT returned to the open browser and clicked on the "START QUIZ" button but at this point did not complete any further questions. The RMIT 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. However, the same notification tab appeared stating that the website was blocked (**Appendix D**).

The RMIT clicked on the button to unblock access and received a warning pop-up prompting it to select an offer. The RMIT clicked on an offer for a "Tesco gift card offer" and later a "Morrisons Gift card", on both occasions the "offers" led the RMIT to the Service landing page.

The RMIT noted that during the monitoring sessions, completing the "offers" resulted in users subscribing to the Service. However, the internet browsers that were blocked by the malware were not unblocked following entry into the Service. The Executive noted 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 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 21 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 a notification on its website stating that the Emergency procedure had been invoked.

The Executive sent a breach letter to the Level 2 provider on 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 2.2.5 – Pricing prominence
- Rule 2.2.2 – Written information material to the decision to purchase
- Paragraph 3.4.1 – Registration of organisation
- Paragraph 3.4.12 (a) – Registration of service

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 did not make any 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 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 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 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 did not make any specific comments in relation to the alleged breach of rule 2.3.1 but made some general remarks. The Level 2 provider confirmed it used affiliate marketing but stated it had not been aware of the malware (ransomware) affiliate marketing promotions described by the Executive. The Level 2 provider asserted that its contracts with affiliate marketers contain stringent terms and conditions that made it clear this type of marketing was prohibited.

   The Level 2 provider asserted that it had investigated the matter and established that a sub-affiliate was responsible for sending the ransomware traffic to the Service landing page. After further investigation the sub-affiliate had discovered that two publishers were responsible for the ransomware traffic. Consequently, these publishers were banned from the platform. The Level 2 provider stated it had worked with its affiliate network and made concerted efforts to find the source of the problem which was demonstrated by extensive written disclosure of message correspondence.

3. The Tribunal considered the evidence and submissions before it. The Tribunal commented that Level 2 providers are responsible for the operation of their services which includes the promotion of a service. Therefore, where a Level 2 provider chooses to engage in affiliate marketing, it will be responsible for any resulting non-compliance. 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:

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

   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 Service was 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 software (**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, despite opting into the Service, the browser remained blocked.

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 the end-user's internet browser would have remained blocked and automatically rerouted to the list of "offers" in an attempt to entice users to opt into the same or another premium rate service. The Executive accordingly asserted that this was highly likely to have misled consumers as they would have been under the impression that, by entering into a further premium rate service, their internet browsers would eventually be unblocked.

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

2. The Level 2 provider repeated the general remarks that it had made in response to the alleged breach of rule 2.3.1. It added that it discusses permitted and prohibited traffic before launching its program via an affiliate network and that its affiliate networks had immediately banned the publishers in question, calling the ransomware promotions "criminal activities".

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 downloading malware and into believing that entering the Service would "unblock" their internet browsers. The Tribunal concluded that there had been a breach of rule 2.3.2 of the Code. Accordingly, the Tribunal upheld a breach of rule 2.3.2 of the Code.

Decision: UPHELD

ALLEGED BREACH 3

Rule 2.5.5

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

1. The Executive submitted that the Level 2 provider 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:

iii. Users' internet browsers being compromised by ransomware and/or
iv. The language used in:
    c. The "WARNING!" pop-up; and
    d. 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 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 users stated "WARNING!" (in a large red bold font). In addition, it stated that the, "The content you are browsing is blocked!" The use of this language, which informed consumers that his/her personal computer functionality had been impaired, was likely to have induced an unreasonable sense of fear, anxiety, distress and/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 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 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 accuses consumers of engaging in "spam bot like" activity which suggests 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 entered 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 submits 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 asserted that it had discussed prohibited promotions with its affiliate networks but it had not seen this particular type of ransomware before. The Level 2 provider reiterated its written submissions made in relation to rule 2.3.1 of the Code and also highlighted that it had not received any complaints in relation to this type of affiliate marketing.

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 2.2.5

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

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

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

   > Paragraph 2.2
   > "As a starting point, pricing information will need to be easy to locate within a promotion (i.e. close to the access code for the PRS itself), easy to read once it is located and easy to understand for the reader (i.e. be unlikely to cause confusion)."
   >
   > Paragraph 2.8
   > "Pricing information where consumers are unlikely to see it, or where it is hard to find, is unlikely to

be judged as 'prominent', or 'proximate', by a PhonepayPlus Code Compliance Panel Tribunal ('PhonepayPlus Tribunal')."

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

The Executive noted that, during the in-house monitoring on 25 June 2013, six screenshots belonging to three different versions of the Service were viewed. Generally, the Executive noted that most of the Service landing pages contained pricing information. However, it was in a small font and the colouring made it unclear and difficult to read. Further, on some pages pricing was not prominent, as it was positioned at the bottom of the page, not presented as standalone information and some distance from the means of access to the Service **(Appendices F and G)**.

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

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

2. The Level 2 provider denied the breach, submitting that pricing was compliant with the Code and the Guidance. The Level 2 provider submitted the pricing was transparent and prominent and made reference to the following:

- At the top of each landing page the text, "Join Triviato quiz subscription service at £4.50 per week. 18+" was stated and there was no need to scroll down to see the pricing.
- The first sentence in the footer text stated the pricing therefore the consumer did not have to read all of the text to find the pricing information.
- The consumer had to indicate that they accepted the terms and conditions before they would subscribe to the Service
- If the terms and conditions were not accepted the pricing was stated on another screen, before they could subscribe to the Service.
- A free text message was sent to the consumer's mobile telephone, which clearly stated the cost of the Service
- Every month, consumers were sent a free text message to notify them of the cost of the Service

The Level 2 provider also stated that, since the launch of the Service, it had run a risk assessment in conjunction with the Level 1 provider to ensure the Service was fully compliant with the Code and Guidance which was evidenced by a risk assessment check provided by the Level 2 provider.

3. The Tribunal considered the evidence and the submissions before it. The Tribunal found the pricing at the top and bottom of the landing pages was in a font which was too small to be considered prominent. In relation to the text at the bottom of the page, the Tribunal noted that the pricing information was not presented as standalone information. On one of the landing pages the pricing

was proximate to the means of entry to the Service but the small size of this pricing, when compared to other items on the page, caused it to be insufficiently prominent and not clearly legible. The Tribunal noted that clear pricing information was generally not proximate to the means of entry to the Service (**Appendices F and G**). Accordingly the Tribunal upheld a breach of rule 2.2.5 of the Code.

Decision: UPHELD

ALLEGED BREACH 5

Rule 2.2.2 Transparency and Pricing

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;
- details of how to leave the service;
- the rules of the quiz;
- the number of prizes;
- the Level 2 provider's identity and contact details;
- participant age restriction; and
- the link to the general terms and conditions.

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

a. the key information, save for the first two 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 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 and stated that it did not agree that consumers were not fully and clearly informed of all key terms.

   The Level 2 provider asserted that it had run a thorough risk assessment in conjunction with the Level 1 provider. During this process the Service landing page, banners and text messages were checked and deemed to be compliant with the Code and Guidance. The Level 2 provider drew the Tribunal's attention to the fact that shortened key terms were included in the same frame that the consumer was required to enter their phone number and formally accept the terms and conditions by ticking a box. The Level 2 provider provided evidence of the written risk assessment.

3. The Tribunal considered the evidence and submissions before it. The Tribunal noted that much of the key information on the Service landing pages was positioned below the fold. The Tribunal concluded that key information, which was material to a consumer's decision to purchase, was not presented in a manner that was easily accessible and clearly legible for the reasons given by the Executive. Accordingly, the Tribunal upheld a breach of rule 2.2.2 of the Code.

Decision: UPHELD

ALLEGED BREACH 6

Paragraph 3.4.1

Before providing any premium rate service all Network operators, Level 1 and Level 2 providers must register with PhonepayPlus subject only to paragraph 3.4.3 below.

1. The Executive asserted that the Level 2 provider had breached paragraph 3.4.1 of the Code on the basis that it had not registered as an organisation on the PhonepayPlus Registration Database.

The Executive commented that it had searched the Registration Scheme database but was unable to locate the Level 2 provider.

The Executive noted that relevant Guidance was published in March 2011 in anticipation of the implementation of the Code in September 2011. In addition, during 2011, and in the build-up to the launch of the new Registration Scheme, PhonepayPlus published numerous registration updates.

Accordingly the Executive submitted that in light of the apparent non-registration, the Level 2 provider had acted in breach of paragraph 3.4.1 of the Code.

2. The Level 2 provider denied that it was in breach of paragraph 3.4.1 of the Code on the grounds that the organisation that "handled" its customer support was registered with PhonepayPlus from 23 December 2011. The Level 2 provider believed that this was sufficient for the purposes of the Code. At the time of registration the Level 2 provider asserted it was not able to register because it did not have a credit card to make payment.

3. The Tribunal considered the evidence and the submissions before it. The Tribunal noted that there was no evidence of the Level 2 provider informing PhonepayPlus of the difficulties caused by the lack of access to a credit card. In any event, the Tribunal commented that alternative payment mechanisms are available. In addition, the Tribunal found that the obligation on Level 2 providers to register is clear under the Code. Consequently, the Tribunal concluded that the Level 2 provider had acted in breach of paragraph 3.4.1 of the Code.

Decision: UPHELD

ALLEGED BREACH 7

Rule 3.4.12(a)

Level 2 providers must provide to PhonepayPlus relevant details (including any relevant access or other codes) to identify services to consumers and must provide the identity of any Level 1 providers concerned with the provision of the service.

1. The Executive initially asserted that the Level 2 provider had acted in breach of paragraph 3.4.12(a) of the Code, as it had failed to register the Service. However, it later transpired that the Service had been registered by the Level 1 provider on the Level 2 provider's behalf. As a result, the Executive withdrew the breach of the Code.

Decision: WITHDRAWN

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 2.2.5 – Pricing prominence
The initial assessment of rule 2.2.5 of the Code was **significant**. In determining the initial assessment for the breach of the Code the Tribunal applied the following criterion:
- The Service was recklessly promoted in such a way so as to impair the consumer's ability to make a free and informed transactional decision.

Rule 2.2.2 – Written information material to the decision to purchase
The initial assessment of rule 2.2.2 of the Code was **serious**. In determining the initial assessment for the breach of the Code the Tribunal applied the following criterion:
- The Service had promotional material that deliberately or recklessly failed to provide consumers with adequate knowledge of the Service and the costs associated with it.

Paragraph 3.4.1 – Registration of organisation
The initial assessment of paragraph 3.4.1 of the Code was **serious**. In determining the initial assessment for the breach of the Code the Tribunal applied the following criterion:
- The Level 2 provider unreasonably failed to register its organisation with PhonepayPlus.

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.

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.
  - Discussions with affiliate networks prior to contracting in relation to permitted and prohibited traffic.
- The Level 2 provider proactively volunteered documentary evidence that had not been prescriptively requested by the Executive, which was material to the Executive's investigation.

Whilst not in itself mitigation, the Tribunal noted that the Level 2 provider had stated it would only re-launch the Service once it is fully compliant with the Code and as such planned to request compliance advice from PhonepayPlus. The Level 2 provider also asserted that it planned to review and reconsider its terms and conditions with its affiliate marketers before the Service recommences operation. The Tribunal also noted that some measures were taken by the Level 2 provider to control and monitor the risks posed by the use of affiliate marketing, but commented that more could still be done to seek out rogue sites in a proactive manner. The Tribunal took into account the detriment suffered by the Level 2 provider as a result of the use of the Emergency procedure.

The Tribunal found that the Level 2 provider's relevant 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. 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

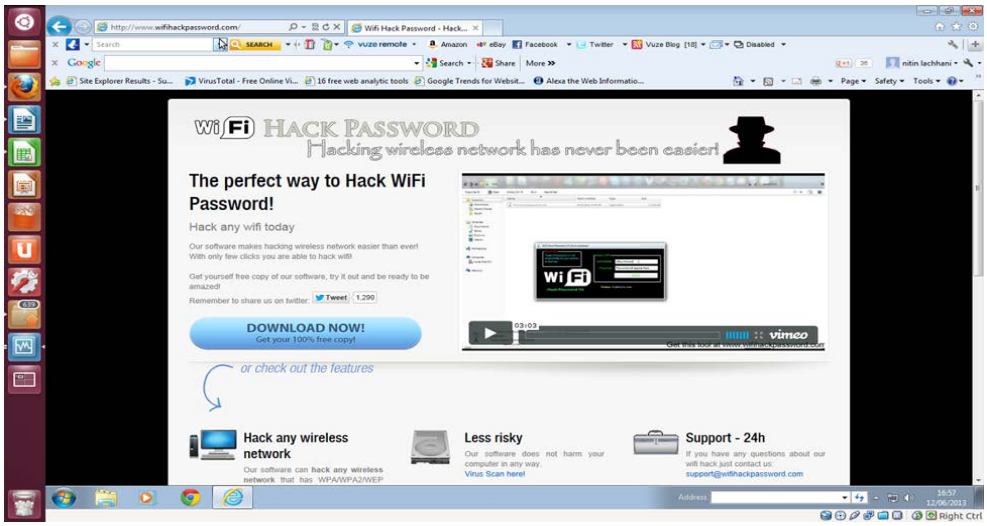
The Tribunal noted that the circumstances of the case were unusual as it was the first time that ransomware had been detected to have been used in the promotion of premium rate services and that there were no complaints. Having regard to all the circumstances of the case, the Tribunal decided to impose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

- a formal reprimand;
- a warning that if the Level 2 provider fails to ensure that it has sufficient measures in place to prevent actual or potential consumer harm being caused by affiliate marketing in future, it should expect to receive a significant penalty for any similar breaches;
- a fine of £27,000; and
- a requirement that the Level 2 provider must refund all consumers who claim a refund, for the full amount spent by them on the Service, within 28 days of their claim, save where there is good cause to believe that such claims are not valid, and provide evidence to PhonepayPlus that such refunds have been made.

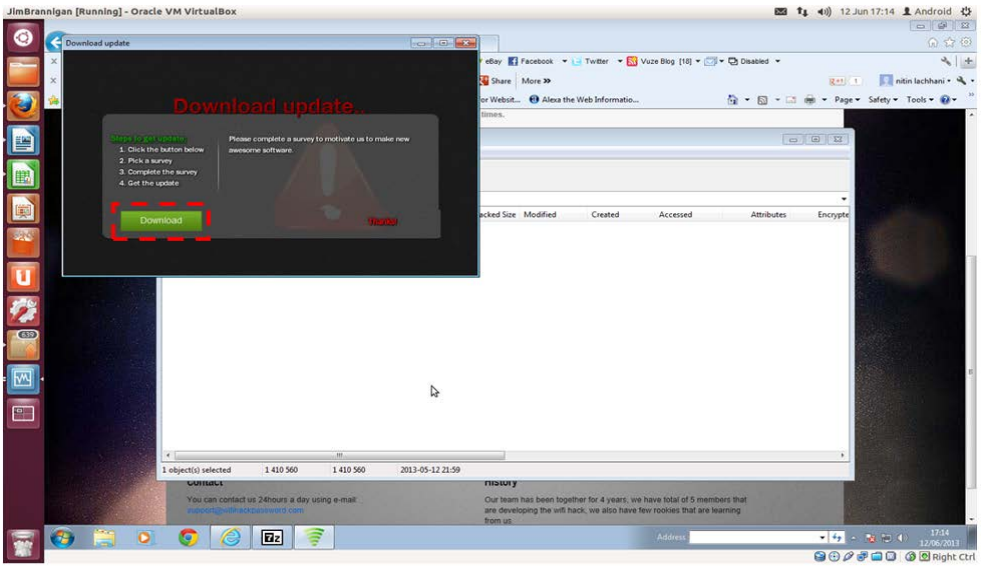
The level of the fine reflected the fact that the Level 2 provider had failed to monitor affiliate marketing for the Service and the additional breaches, which indicated a broader failure in relation to its compliance with the Code.

Appendices

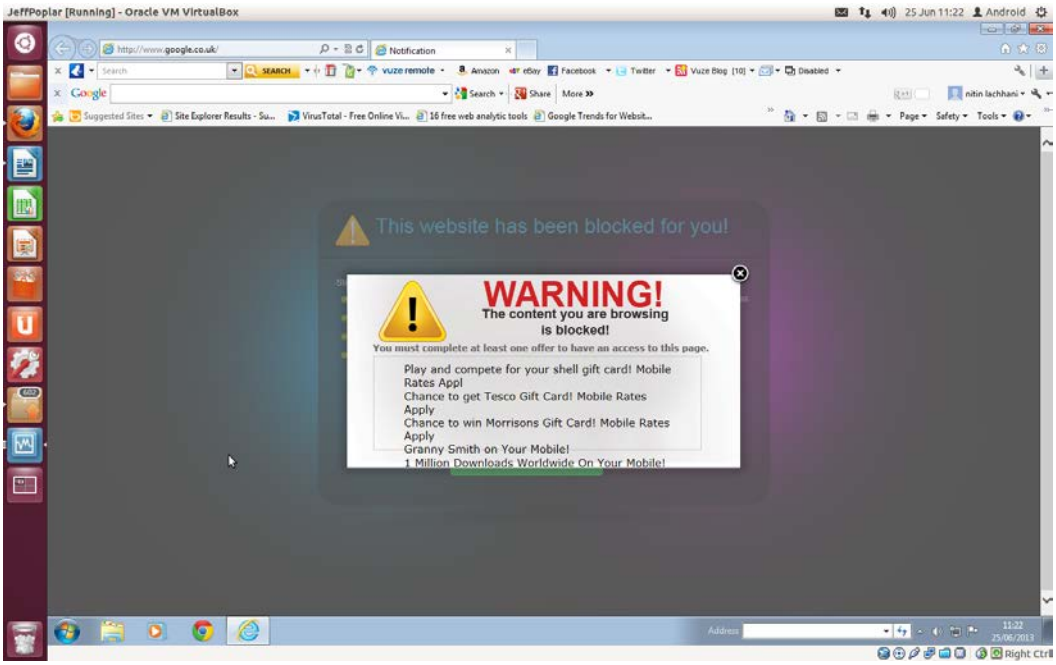
Appendix A: Screenshot of Wifihackpassword.com:



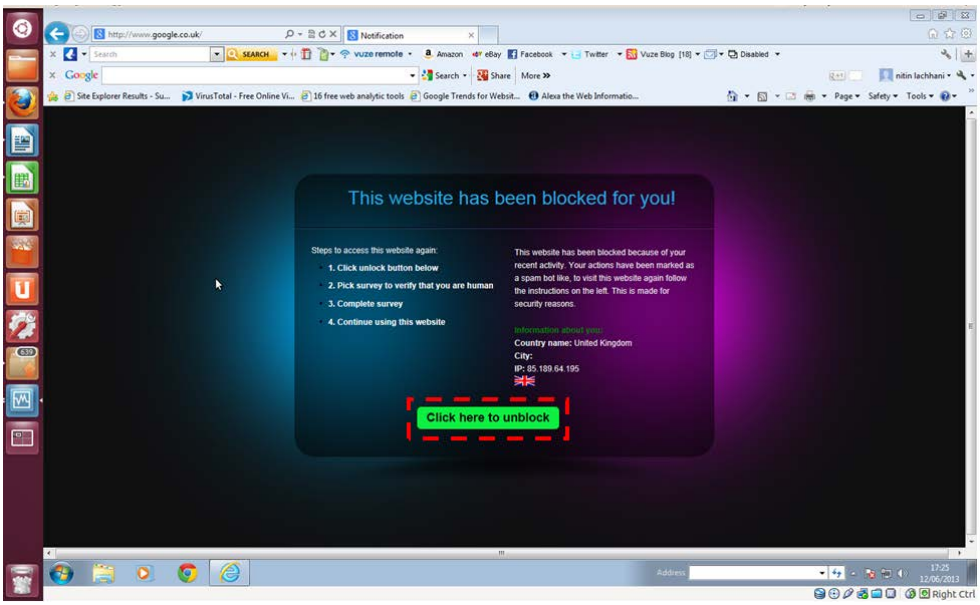
Appendix B: Screenshot including the dialogue box offering an update:



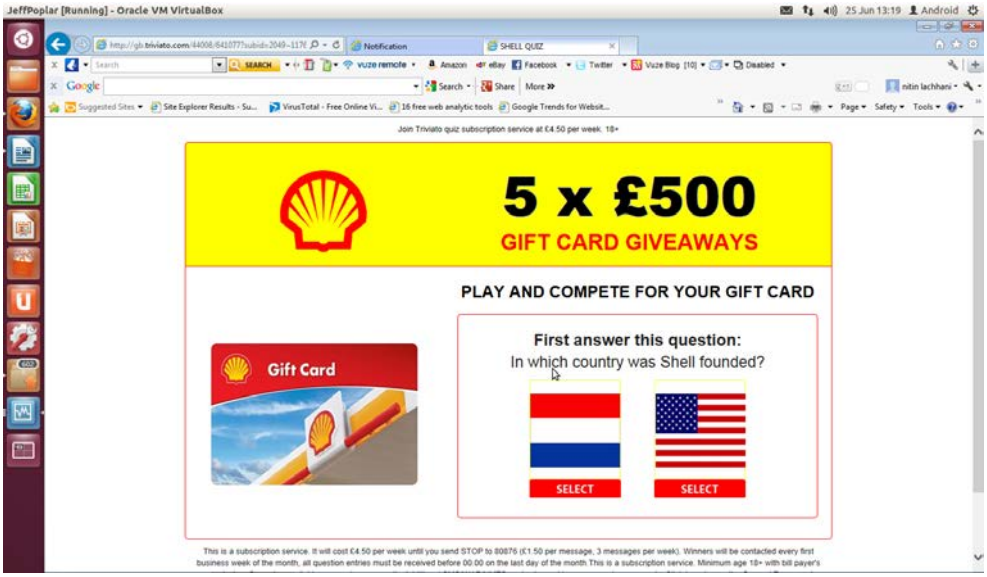
Appendix C: Screenshot of the “Warning” webpage:



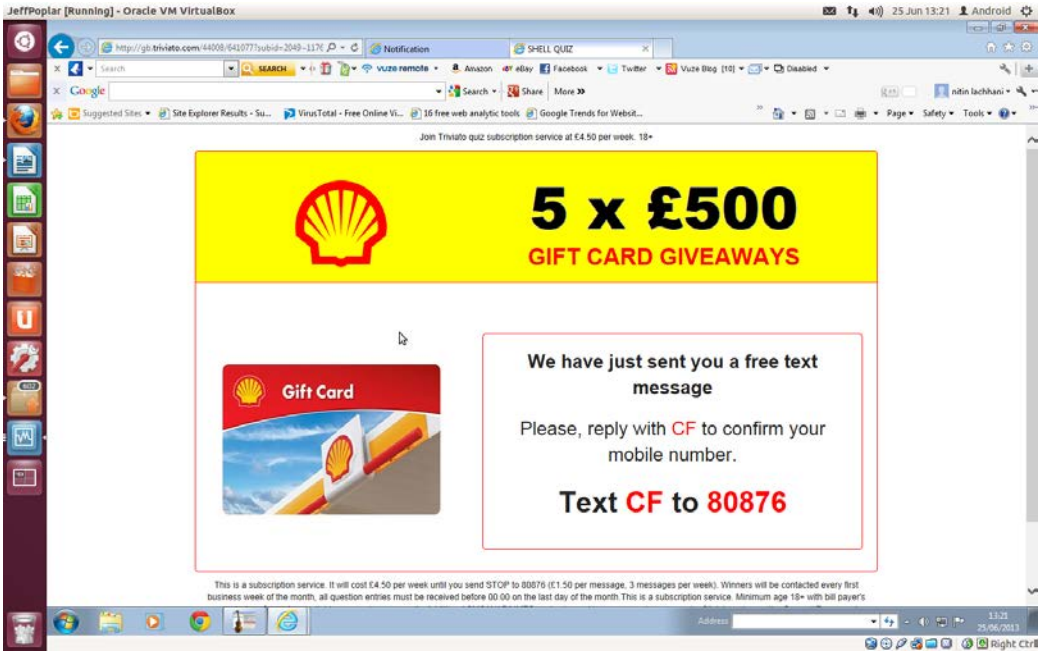
Appendix D: Screenshot of “spam bot” warning:



Appendix E: Screenshot of the "Shell Gift Card Giveaway" Service landing page:



Appendix F: Screenshot of the "Shell Gift Card Giveaway" subscription opt in webpage:



Appendix G: Screenshot of the "Morrisons Gift Card Giveaway" subscription opt in instructions: