Tribunal Sitting Number 130 / Case 2

Case Reference: 28791

Level 2 provider	Bafona Ltd
Type of Service	Competition - non-scratchcard
Level 1 provider	txtNation Limited and OpenMarket Limited
Network operator	All Mobile Network operators

THIS CASE WAS BROUGHT AGAINST THE LEVEL 2 PROVIDER UNDER PARAGRAPH 4.4 OF THE CODE

BACKGROUND

The Level 2 provider, Bafona Ltd operated an online subscription competition quiz service, "Zovut" (the "**Service**"). The Service was operated using Payforit ("**PFI**") at a cost of £4.50 per week and was promoted via affiliate marketing. The Level 1 providers for the Service were txtNation Limited and OpenMarket Limited.

The Service offered consumers the opportunity to participate in weekly quiz competitions. Consumers who answered the most questions correctly in the shortest time period won a prize (prizes were awarded on a monthly basis, such as, an X-Box 360).

The Service operated from 12 June 2013 to 2 July 2013 (when it was suspended as a result of the use of the Emergency procedure).

PhonepayPlus received no complaints from consumers. Concerns regarding the promotion of the Service were uncovered as a result of in-house monitoring conducted by the PhonepayPlus Research and Market Intelligence Team (the "**RMIT**"). The monitoring revealed that affiliate marketing, which generated consumer traffic to the Service, appeared to utilise a form of malware that stopped users' internet browsers working, and resulted 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, the RMIT visited the website "wifihackpassword.com" (**Appendix A**), which offered users software that purported to enable them to hack into locked Wi-Fi networks. The RMIT clicked on a button marked "Download Now!" which resulted in a file being downloaded. The RMIT opened the file, instantly a dialogue box appeared and offered a seemingly essential update which the RMIT declined (**Appendix B**). After the RMIT clicked "No", a further dialogue box appeared which stated (**Appendix C**):

> "Error! Too old version Update please!"

The only option to click was "OK". After the RMIT clicked on "OK", the dialogue box closed. The RMIT then closed all open windows and attempted to open the Google Chrome browser. The RMIT found the homepage blocked (**Appendix D**). The webpage displayed the following message:

> "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."

After the RMIT clicked on "Click here to unblock", a further pop-up appeared which stated (**Appendix E**):

> "WARNING! The content you are browsing is blocked! You must complete at least one offer to have access to this page."

The RMIT selected an option that stated "Win XBOX 360". The RMIT was subsequently directed to the Service operated by the Level 2 provider in a new browser window (**Appendix F**). The RMIT followed the instructions contained on the landing page and was directed to the PFI screen which requested a MSISDN. The RMIT did not enter a MSISDN.

The Executive asserted that had the RMIT entered a MSISDN, it would have been sent a free message containing a keyword, and instructions to send the keyword to the Service shortcode in order to subscribe to the Service.

The Executive relied upon previous monitoring conducted by the RMIT through the same affiliate marketing route. During these monitoring sessions, and despite following all instructions and subscribing to a number of different premium rate services, the RMIT's internet browser remained "blocked". It was therefore submitted that, had the RMIT subscribed to the Service, the outcome would have been the same as experienced in previous monitoring sessions and the browser would have remained blocked.

On 25 June 2013, the RMIT opened the Internet Explorer browser to find that its homepage (google.co.uk) was blocked (**Appendix D**). The Executive noted that a message stated that the homepage was blocked due to "spam bot" activity. The Executive submitted that this statement was false, and that in reality the homepage was blocked due to the initial file download from "Wifihackpassword.com".

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 Code Compliance Panel ("**CCP**") member and sought authorisation to invoke the Emergency procedure in relation to the Service pursuant to paragraph 4.5.2 of the Code. The CCP member considered the

seriousness and urgency of the case and determined that the Emergency procedure should be used. The outcome was communicated to the Level 1 provider along with a direction to suspend the Service on 1 July 2013. The Level 1 provider confirmed suspension of the Service on 1 July 2013. The Executive informed the Level 2 provider of its monitoring and the use of the Emergency procedure on 2 July 2013 (due to uncertainty in relation to the identity of the Level 2 provider).

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.

The Executive sent a breach letter to the Level 2 provider on 5 July 2013. Within the breach letter the Executive raised the following breaches of the Code:

- Rule 2.3.1 – Fair and equitable treatment
- Rule 2.3.2 – Misleading
- Rule 2.5.5 – Avoidance of harm (fear, anxiety, distress or offence)
- Paragraph 3.4.12(a) – Registration of Service

The Level 2 provider responded on 10 July 2013. On 11 July 2013, the Level 2 provider supplied additional information in relation to the investigation. On 25 July 2013, the Tribunal reached a decision on the breaches raised by the Executive.

SUBMISSIONS AND CONCLUSIONS

PRELIMINARY ISSUE

Responsibility for affiliate marketing

The Tribunal noted that Level 2 providers are responsible for the Services that they operate; this includes how the services are promoted.

Part 2 of the Code states:

> "References to a premium rate service…include all aspects of a service including content, promotion and marketing…Level 2 providers have responsibility for achieving these outcomes by complying with the rules in respect of the provision of the relevant premium rate service."

Paragraph 5.3.8(b) states:

> "A Level 2 provider is the person who controls or is responsible for the operation, content and promotion of the relevant premium rate service and/or the use of a facility within the premium rate service."

Further, Code paragraph 5.3.29 states:

> "'Promotion' means anything where the intent or effect is, either directly or indirectly, to encourage the use of premium rate services, and the term 'promotional material' shall be construed accordingly."

As a result, the Tribunal found that the Level 2 provider was responsible for the ransomware affiliate marketing promotions which led to the Service landing pages.

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 had 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 above. The Executive noted that the Service was promoted using affiliate marketing that resulted in users downloading ransomware (a type of malware). The ransomware blocked users' internet browser functionality. Users then entered the Service incurring premium rate charges in order to unblock their browsers.

The Executive asserted that the malware that blocked users' internet browser functionality interfered with their computers and had the potential to cause inconvenience and unnecessary costs. The Executive asserted that, as a result of the ransomware, users were not treated fairly and equitably.

Additionally, the promotion for the Service attempted to force users into entering into the 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 accepted that it was responsible under the Code for the actions of its affiliate marketers and the content of their promotions. It added that the acts of the affiliate marketer were, "malicious and purely fraudulent", and had affected a number of other providers. It contended that:

> "….. [T]he attacker was not an affiliate trying to make some quick money, this appears to be targeted towards specific companies providing specific services."

The Level 2 provider set out full details of the party that it believed to be responsible for the

malware promotions.

The Level 2 provider stated that it did not allow or authorise the malware promotion and that the affiliate marketing promotion was illegal and violated users' privacy. It submitted that it immediately terminated the responsible affiliate marketer and also filed a complaint with PayPal, who the affiliate used to receive payments.

It also stated that:

> "The promotion goes against all our agreements, we understand that its [sic] our responsibility to ensure compliance from affiliate marketers, however in this incident we have been mislead *[sic]* and misguided by an affiliate operating with bad intent, we hope for the understanding of PhonePayPlus *[sic]* when deciding the upon *[sic]* intentions of the breach."

The Level 2 provider submitted that it had found that the responsible affiliate network sent 158 subscribers to the Service. Three of the subscribers experienced the same ransomware journey as the RMIT. The Level 2 provider stated that it intended to refund every user who had come to the Service from this affiliate in full.

In conclusion, the Level 2 provider accepted that there had been a breach of rule 2.3.1 of the Code as users were not treated fairly and equitably. However, it asserted that it was a, "victim just like the users who signed up for the service unwillingly".

3 The Tribunal considered all the evidence and submissions before it. The Tribunal noted that the Level 2 provider accepted that a breach of rule 2.3.1 of the Code had occurred and that it was responsible under the Code. The Tribunal commented that Level 2 providers are responsible for the operation of their services, which includes the promotion of a service. Therefore, where a Level 2 provider chooses to engage in affiliate marketing, it accepts the risk that any affiliate marketing outside its direct control may lead to non-compliance for which it is responsible. Consequently, and for the reasons given by the Executive, the Tribunal concluded that consumers had not been treated fairly and equitably, as a result of the malware affiliate marketing promotion, in breach of rule 2.3.1 of the Code. Accordingly, the Tribunal upheld a breach of rule 2.3.1 of the Code.

Decision: UPHELD

ALLEGED BREACH 2

Rule 2.3.2

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

1 The Executive submitted that the Level 2 provider 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 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 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:

"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 affiliate marketing

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 noted that it was highly likely that users would have been led to believe that they were required to complete a "survey" (which actually transpired to be the subscription process for the Service) in order to download the Wi-Fi hacking file (**Appendix D**).

Further, on discovering that its browser had been blocked and having clicked, "Click here to unblock" (**Appendix D**) the RMIT was given a "WARNING!" notification which stated that its internet browser content had been "blocked", and, in order to unblock the browser, it was required to complete at least one "offer". The RMIT clicked on an "offer" which led to the Service landing page. The RMIT did not enter a MSISDN.

The Executive relied on earlier monitoring of the malware affiliate marketing promotion carried out by the RMIT (detailed in the "Background" section above). During the earlier monitoring the RMIT subscribed to a different premium rate service and yet its browser

remained blocked.

The Executive submitted that the totality of the monitoring demonstrated a carousel of aggressive affiliate marketing. Therefore, the Executive submitted that had the RMIT opted into the Service, it would have encountered the same experience and the browser would have 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 Executive accordingly asserted that this was again 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 evidence the Executive submitted that the Level 2 provider had acted in breach of rule 2.3.2 of the Code and outcome 2.3 had not been achieved.

2 The Level 2 provider accepted that consumers had been misled by the affiliate marketing promotion but asserted that the affiliate marketer had acted with, "bad intent or intent to harm". The Level 2 provider appealed to the Tribunal to treat it with "fairness and mercy" and stated that it had fully co-operated with PhonepayPlus and would provide any data in its possession to law enforcement personnel.

The Level 2 provider reiterated that it was responsible under the Code for actions of affiliate marketers but that the actions of the affiliate had been:

> "[M]alicious and purely fraudulent, especially considering the fact that, "the attacker did not even repair the users' computers after the steps explained were completed".

Finally, the Level 2 provider stated that it did not condone the actions of the affiliate marketer and that it was unaware of the actions until being notified by PhonepayPlus.

3 The Tribunal considered all the evidence and submissions before it. The Tribunal noted that the Level 2 provider accepted that a breach of rule 2.3.2 of the Code had occurred and that it was responsible under the Code. The Tribunal commented that Level 2 providers are responsible for the operation of their services, which includes the promotion of a service. Therefore, where a Level 2 provider chooses to engage in affiliate marketing, it accepts the risk that any affiliate marketing outside its direct control may lead to non-compliance for which it is responsible. Consequently, and for the reasons given by the Executive, the Tribunal concluded that consumers 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 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:

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 details of the monitoring of the Service set out in the "Background" section above.

The Executive noted that the Service was promoted via affiliate marketing. As set out in the "Background" section above, 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 E)

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 and 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 or offence as they may have reasonably 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 a breach of rule 2.5.5 of the Code had occurred and outcome 2.5 had not been satisfied.

2 The Level 2 provider accepted that there had been consumer harm involved in the promotion of the Service and further stated that it would rectify the consumer harm by refunding every user directed from the affected affiliate marketer, regardless of whether or not the user complained about it.

The Level 2 provider submitted that the promotion was done by a non-compliant affiliate marketer who was not "normal" and had bad intentions. It commented that the affiliate marketer had caused harm to both the businesses running the Services and the consumers using the Services.

The Level 2 provider submitted that refunding all users in full would cause it a substantial loss as each refund:

> " [W]ill be about 50% more than we get paid [which] is already a very harsh punishment for a new service that is just started. We hope the executives will take this into consideration when deciding on its breaches and if we are the victim or the beneficiary of this scam."

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

sense of anxiety and distress in breach of rule 2.5.5 of the Code. Accordingly, the Tribunal upheld a breach of rule 2.5.5 of the Code.

Decision: UPHELD

ALLEGED BREACH 4

Paragraph 3.4.12(a)

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

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

The Executive noted that the Level 2 provider had failed to register the Service (including the Service name) on the PhonepayPlus Registration Database. In addition, the Executive noted that PhonepayPlus had published a large amount of information in relation to providers' registration obligations under the Code prior to it coming into force in September 2011.

The Executive accordingly submitted that, for the reason outlined above, the Level 2 provider had acted in breach of paragraph 3.4.12(a) of the Code.

2 The Level 2 provider denied the breach, asserting that it had registered the Service. It provided the reference, "ORG832-37260-42979" as proof of registration.

3 The Tribunal considered the evidence and noted that the Level 2 provider had provided evidence that it had registered its organisation on the PhonepayPlus Registration Database. However, the Tribunal found that the Level 2 provider had failed to register the Service as required by paragraph 3.4.12(a) of the Code. The Tribunal noted that the requirement to register a service is an important obligation as non-registration results in consumers not being able to ascertain the details of a service on the Number Checker. Accordingly, the Tribunal upheld a breach of paragraph 3.4.12(a) of the Code.

Decision: UPHELD

SANCTIONS

Initial Overall Assessment

The Tribunal's initial assessment of the breaches of the Code was as follows:

Rule 2.3.1 - Fair and equitable treatment

The initial assessment of rule 2.3.1 of the Code was **very serious**. In determining the initial assessment for this breach of the Code the Tribunal applied the following criteria:

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

Rule 2.3.2 - Misleading

The initial assessment of rule 2.3.2 of the Code was **very serious**. In determining the initial assessment for this breach of the Code the Tribunal applied the following criteria:

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

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

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

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

Paragraph 3.4.12(a) – Registration of a service

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

- The Level 2 provider negligently failed to comply with the requirement to register the Service.

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 measure in place to identify and mitigate against the risks associated with affiliate marketing:
  - Contracts with its affiliate marketing partners, which provided for certain traffic restrictions, including the avoidance of illegal content.
- The Level 2 provider stated that it intended to contact 153 consumers who had accessed the Service through the non-complaint affiliate marketer to offer them a refund.
- The Level 2 provider disclosed details including the IP, address and the bank details of the affiliate marketer behind the breaches. It also stated that it had reported the affiliate marketer to PayPal as well as to the police in the USA, United Kingdom and Estonia.

The Tribunal commented that the weight to be given to the mitigating factors had to be balanced against the failure to have sufficient measures in place to control and monitor the risk posed by the use of affiliate marketing. However, the Tribunal took into account the detriment suffered by the Level 2 provider as a result of the use of Emergency procedure.

The Tribunal found that the Level 2 provider's relevant revenue in relation with the Service was in the range of Band 6 (£1 - £5,000).

The Tribunal noted that the Service and the Level 2 provider's landing pages were not predicated on fraudulent activity, that the Service had some value and that a large part of the Level 2 provider's revenue appeared to be from legitimate sources. However, having taken into account the aggravating and mitigating factors, the Tribunal concluded that the seriousness of the case should be regarded overall as **very serious.**

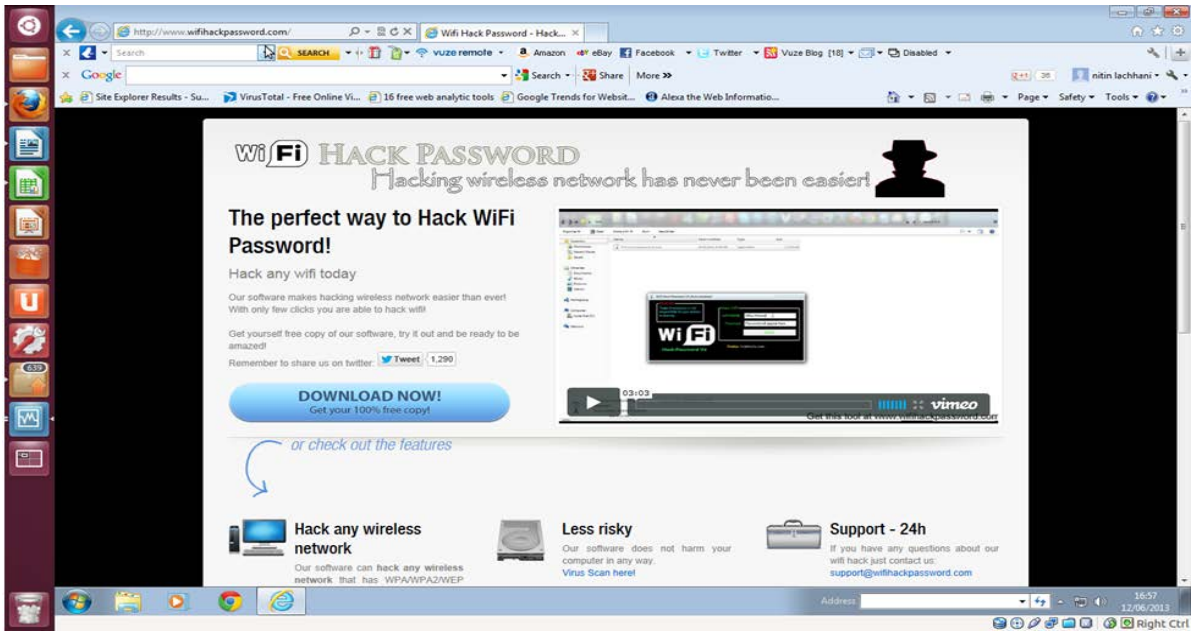
Sanctions Imposed

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

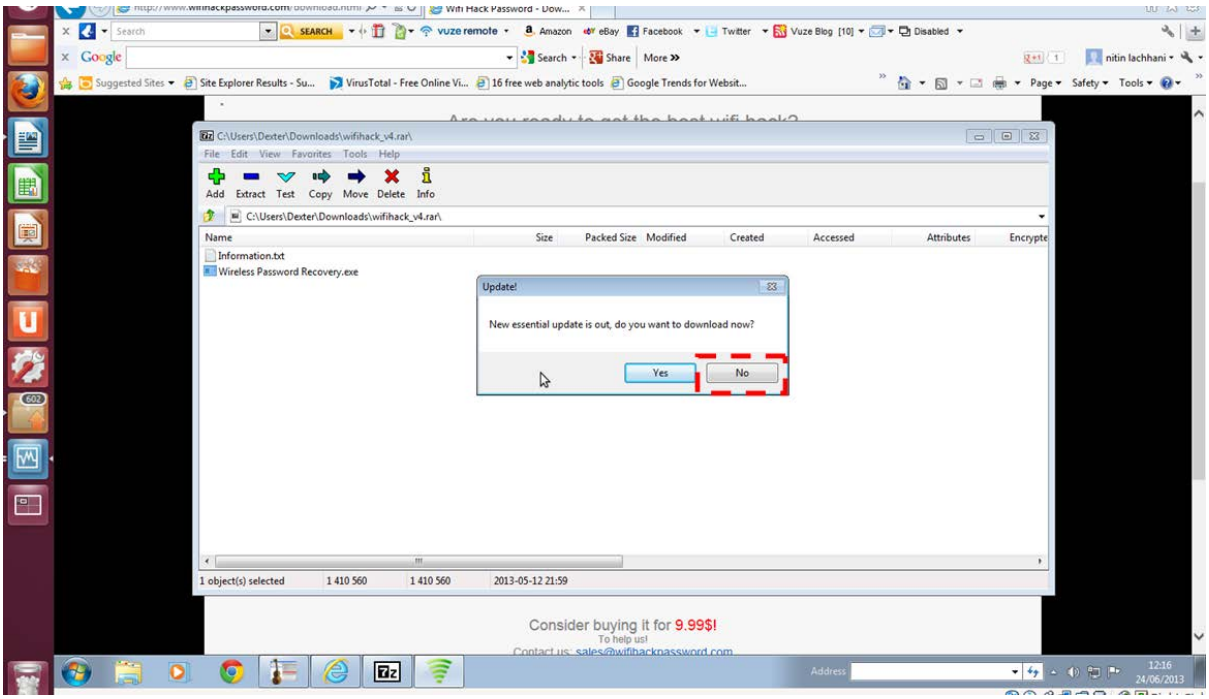
- a formal reprimand;
- a warning that if the Level 2 provider fails to ensure that it has sufficient measures in place to prevent actual or potential consumer harm being caused by affiliate marketing in future it should expect to receive a significant penalty for any similar breach;
- a fine of £25,000; and
- a requirement that the Level 2 provider must refund all consumers who claim a refund, for the full amount spent by them on the Service, within 28 days of their claim, save where there is good cause to believe that such claims are not valid, and provide evidence to PhonepayPlus that such refunds have been made.

Appendices

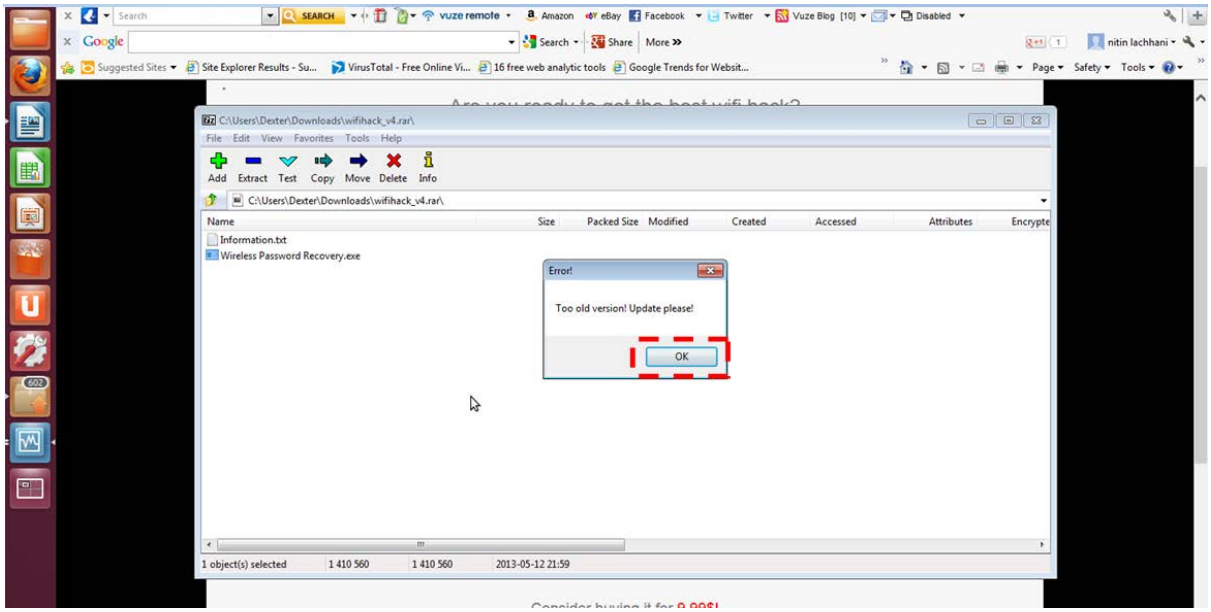
Appendix A: Screenshot of www.wifihackpassword.com:



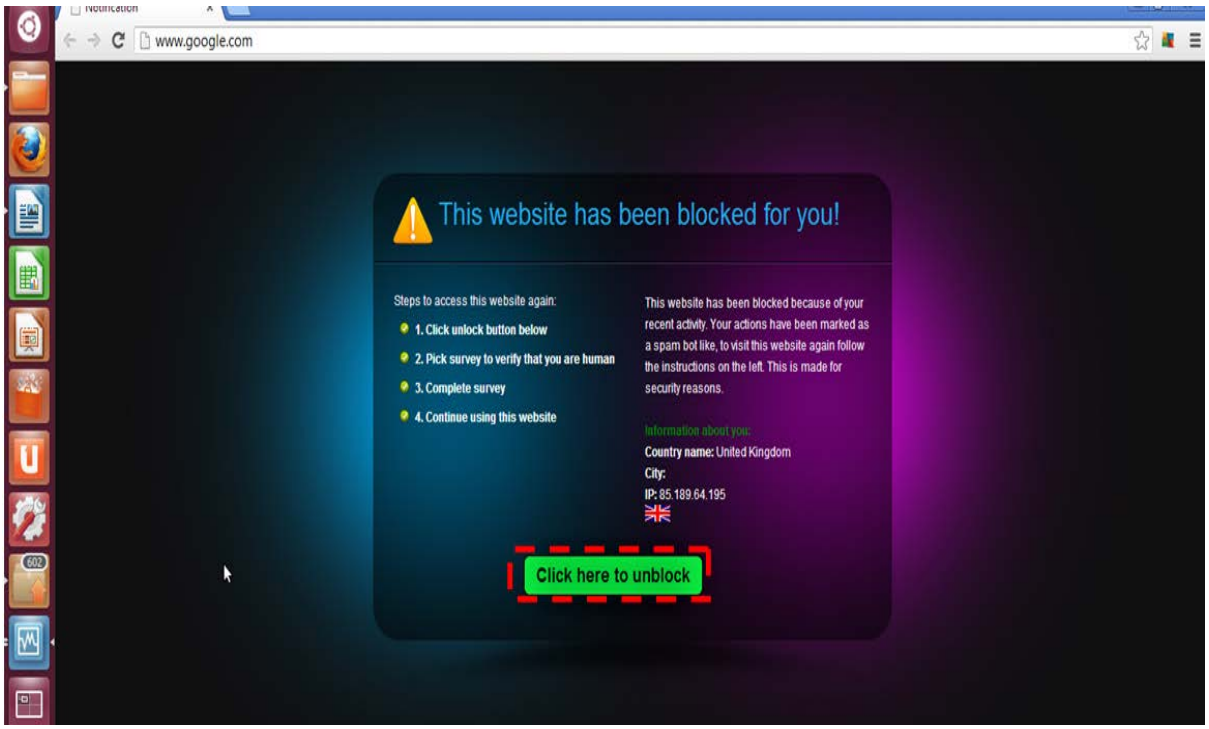
Appendix B: Screenshot of the "essential update" dialogue box:



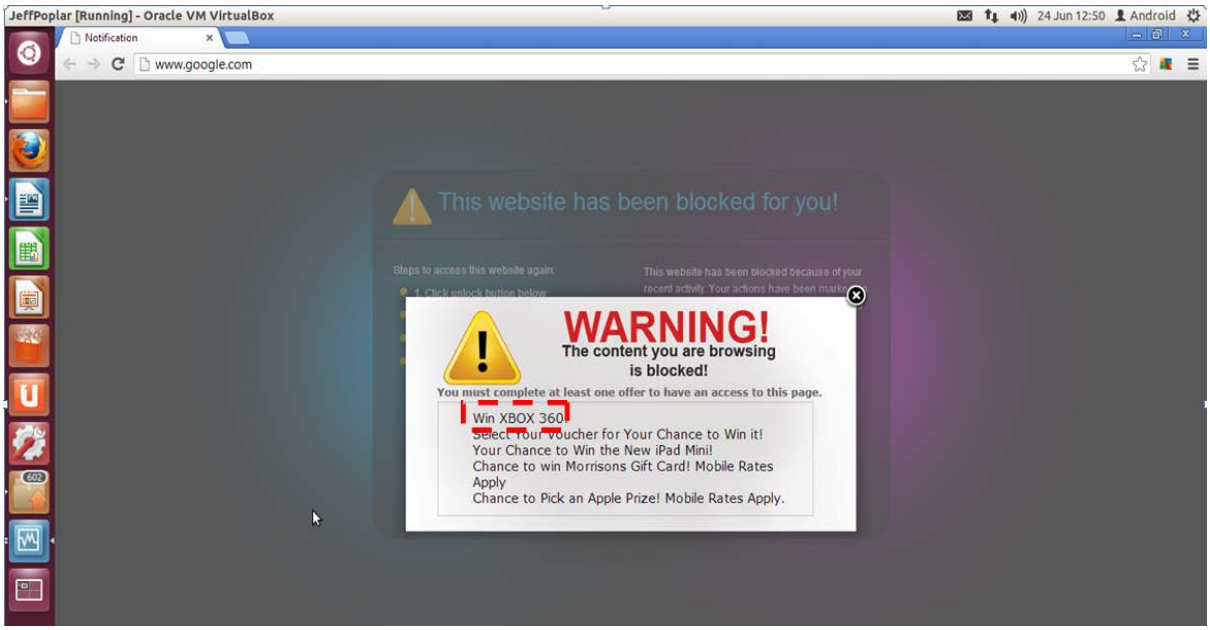
Appendix C: Screenshot of "Error! Too old version! Update please!" dialogue box:



Appendix D: Screenshot of the "spam bot" warning:



Appendix E: Screenshot of the “Warning” pop-up:



Appendix F: Screenshot of a Service webpage: