

**PHONEPAYPLUS LIMITED**

**Executive**

**and**

**BITSTACKER LIMITED**

**Respondent**

---

---

**ORAL HEARING DECISION**

---

---

**Tribunal members:**      **Linda Lee (Chair)**  
   **Peter Hinchcliffe**  
   **Elizabeth Ribbans**

**DECISION**

Upon an application for an oral hearing by Bitstacker Ltd (“Bitstacker”) under paragraph 3.1 of Annex 2 of the PhonepayPlus Code of Practice (12<sup>th</sup> edition) (“the Code”):

1. Bitstacker breached paragraphs 2.3.1, 2.3.2 and 2.5.5 of the Code in that the promotion of its service through the website [www.wifihackpassword.com](http://www.wifihackpassword.com) and associated malware failed to treat consumers of premium rate services fairly and equitably, was likely to mislead, and was likely to induce an unreasonable sense of fear, anxiety, distress and offence in consumers.
2. Bitstacker was not in breach of paragraph 2.3.2 of the Code in relation to the promotion of its service through the website [www.lottobytext.co.uk](http://www.lottobytext.co.uk), because this promotion was not likely to mislead.
3. The sanctions determined by the Oral Hearing Tribunal (“the Tribunal”) are:

- 3.1. a formal reprimand;
  - 3.2. a fine of £25,000.
4. Under paragraph 4.10.1 of the Code, the Tribunal recommends that Bitstacker be required to pay 90% of the relevant administrative charge.

## **REASONS**

1. The oral hearing relating to this case took place on 13 December 2013 and 3 February 2014. At the hearing the PhonepayPlus Executive (“the Executive”) was represented by Mr Selman Ansari of Bates, Wells & Braithwaite. Bitstacker was represented by Mr Kieron Beal QC of counsel. Ms Arpan Boyall and Mr Nitin Lachhani of the Executive and Mr Mark Lewis and Mr Derick Peters of Bitstacker gave oral evidence. The clerk to the Tribunal was Mr Alexander Macpherson of counsel.

### **Description of the services and their promotion**

2. Bitstacker operates a website called [www.lottobytext.co.uk](http://www.lottobytext.co.uk) which offers a mobile telephone text message service providing the National Lottery and Euromillions results together with a mobile telephone based lottery syndicate service. Customers register for the service on the website and pay by text message. They are charged £1.50 per Lotto draw, or £4.50 for entry into 3 draws per week. Bitstacker manages the promotion of the service, the billing and the delivery of the information via text message. Bitstacker’s service is a premium rate service and Bitstacker is a Level 2 provider for the purposes of the Code.
3. This case involves the decision by Bitstacker to market the lottobytext service through networks of ‘affiliates’, who were to be rewarded with a commission payment if they directed potential users of the service to Bitstacker’s website and who were largely free to select the content of their promotion. In this case the Executive’s concern relates to the alleged promotion of Bitstacker’s service through the website [www.wifihackpassword.com](http://www.wifihackpassword.com) by unknown third parties. In June 2013 the Executive became aware of a link between this website, which purported to offer a free download of software which would enable users to hack password-protected wireless networks, and the lottobytext service. The software downloaded from the website did not in fact permit such access. Instead, the software downloaded was a form of ‘ransomware’, which had the effect of blocking users from opening

their internet browser and/or from accessing popular websites. The user would initially encounter a message stating that the website had been blocked together with a dialogue box labelled "*click here to unblock*". Clicking on this box generated the following message:

*"WARNING!*

*The content you are browsing is blocked!*

*You must complete at least one offer to have an access to this page."*

4. When the Executive monitored this website in June 2013 there were five links to 'offers' below this message, the first of which stated: "*Could you be the next millionaire? Mobile Rates. Appl.*" Clicking on this link took the user to the website [www.lottobytext.co.uk](http://www.lottobytext.co.uk) which promoted Bitstacker's service.
5. Following the link to the lottobytext website, or even subscribing to Bitstacker's service once there, did not in fact have the effect of unblocking the user's internet browser. This required remedial action of some technical sophistication taken in respect of the computer's settings.
6. There was no issue between the parties at the hearing that the arrangements set out above relating to the wifihackpassword website were misleading, malicious and illegal, although there was a difference of view as to the likely intent of those responsible. It was also not disputed that Bitstacker did not itself create, instigate or have any knowledge of the wifihackpassword website and its operation prior to their being drawn to its attention by the Executive. At issue was whether the link to the lottobytext website constituted a promotion of Bitstacker's service and whether Bitstacker could be held accountable for the same under the Code.
7. The service was operational from 15 May 2013 until it was suspended by reason of an Emergency Procedure (under section 4.5 of the Code) on 2 July 2013. Following a review tribunal on 4 July 2013, the service resumed from 10 July 2013 subject to various conditions, including a condition that no online affiliate marketing would be undertaken. The chair of the Tribunal subsequently lifted this condition on 7 November 2013 by consent between the parties.

8. The hearing also related to the promotion of Bitstacker's service through its lottobytext website. On the website, the service is described as being "*the smart way to play the lottery*". A promotional offer is also made by means of which consumers are told they can "*get 5 free Euromillions/Lotto lines on your mobile*".

**Oral evidence considered by the Tribunal**

9. In her witness statement, Ms Boyall referred to the monitoring of affiliate marketing leads offered by a company called Adscend Media LLC ("Adscend"). Documentation showed that payment for leads generated to Bitstacker's service was being offered by Adscend at the relevant time, suggesting that Adscend was an affiliate marketer with indirect contractual links to Bitstacker which would permit it to claim and receive payment for such leads.
10. Ms Boyall also stated that her analysis of the probability of winning a lottery jackpot through Bitstacker's service indicated that this was not in fact "*the smart way to play the national lottery*". She stated that a consumer would be better off purchasing lottery tickets directly.
11. Ms Boyall also stated that the prominent offer "GET 5 FREE EUROMILLIONS/LOTTO LINES ON YOUR MOBILE" was likely to mislead, because in fact consumers were required to subscribe to a charged service in order to get these 'free' entries.
12. Mr Lachhani is a Research Market Intelligence Executive employed by the Executive and he was the individual whose monitoring revealed the ransomware associated with the wifihackpassword website. He states in his witness statement that when he clicked on the link which was stated would unblock the computer, an Adscendmedia.com URL and a Filefire.org URL were displayed in the brief moment while the redirection to the lottobytext website was taking place. He made a contemporaneous note of this, but was unable to capture this by means of a screenshot because it happened so quickly. In his haste, he recorded the Filefire.org URL as Filefire.com.
13. Online research showed that the largest number of destination sites to which Filefire.org directed services were through Adscend. Thus Adscend was a customer for the traffic generated by Filefire.org. Further evidence from a website called [www.similarweb.com](http://www.similarweb.com) suggested that the greatest referrer of traffic to the lottobytext website was Adscend. Mr Lachhani stated that this did not necessarily mean that there was a direct contractual

arrangement between Bitstacker and Adscend, as the traffic flow arrangement could have been made by a third party advertising agent. He considered it highly unlikely that the use of filesharing sites and publishers of this nature would be motivated by anything other than the desire to generate revenue from the promotion of services.

14. Mr Lachhani was sceptical of the theory put forward on behalf of Bitstacker that the wifihackpassword website could have been intended to gather unauthorised information from consumers. He did not detect any sophisticated malware of this type when he applied virus detection software, and he concluded that it appeared to be a standard piece of malware.
15. In oral evidence, Mr Lachhani confirmed that it was simply impossible to capture the URLs on redirection by means of a screenshot, but he confirmed that he had seen the relevant URLs and had made a contemporary note. On this basis he stated that Adscend must have been in the value chain between the operators of the wifihackpassword website and Bitstacker.
16. Mr Lachhani accepted, however, that if Bitstacker's suggestion that the link in question came from a promotional email campaign (and thus did not contain the relevant code which would trigger the right to the payment of commission) was correct, then there could not have been a potential financial link between the operators of the wifihackpassword website responsible for the ransomware and Bitstacker.
17. He also stated that he could find no evidence that the ransomware was geared towards data collection. He stated that he would expect such a data collection operation to be a highly covert one, and he considered it unlikely that if this had been the purpose of the malware it would have advertised its presence so clearly.
18. The Executive relied upon posts on an internet marketing forum by a Mr Patel of Bitstacker. It was contended that these demonstrated that Bitstacker was actively pursuing the deployment of content-locking as a promotional tool.
19. Mr Lewis is the managing director of Bitstacker. In his witness statement, he stated that Bitstacker has never had any relationship, knowledge of or dealings with Adscend. He stated that when alerted to the problem by the Executive, Bitstacker was able to establish that the link used by the malware to access the lottobytext website was not associated with any

incentivised affiliate codes, but related to one of Bitstacker's own promotional emails. A print out of the relevant email promotion was provided, which had the URL which Bitstacker said had been returned by those referred from the wifihackpassword website pasted alongside it.

20. Mr Lewis contended that the malware was not a promotion mechanic for Bitstacker's service but rather was probably intended to be a means of collecting unauthorised personal data. He relied upon a report from a cybercrime expert which Bitstacker had commissioned to support this contention.
21. Mr Lewis pointed out that Bitstacker's business model requires subscribers to remain subscribed beyond 2 months, as it is only at this point that Bitstacker starts getting a return on its investment. It would be nonsensical to target potential criminals (who were seeking to download illegal hacking software) and force them to join a service against their will. Further, Bitstacker delays payment to affiliates for 30 days, so that it can review the quality of the registrations provided. Any traffic generated by the wifihackpassword site would not deliver conversions of any value to Bitstacker.
22. In his oral evidence, Mr Lewis stated that the lottobytext website would ask for personal information and credit card details. Intercepting such information would have been the primary purpose of the malware. He accepted that the evidence demonstrated that there was an indirect link between Adscend and Bitstacker, although Bitstacker had not been aware of this at the time.
23. Mr Lewis stated that Bitstacker had not retained any documentary evidence demonstrating that the referral code linked to the wifihackpassword related to the email promotion referred to. Bitstacker only kept such data for 14 days and it had not been retained. He did not know when the relevant email campaign had been, and Bitstacker was only able to produce a generalised email as the finished emails had not been stored.
24. Mr Lewis stated that only 9 individuals had been referred to the lottobytext website from the wifihackpassword website, and none of these had in fact subscribed to the service.
25. Mr Lewis accepted that Bitstacker's contracts with affiliates did not, and still do not, require the affiliates to give details of the sub-affiliates which they contract with.

26. Mr Peters is a shareholder of Bitstacker who plays an integral role in the day to day running of the business. He stated that the 'smart way to play' has been the business' prominent website strapline certainly since 2008. The Executive will have been aware of it since then in connection with its investigation into the former operators of the business, Marketing Craze Limited.
27. In oral evidence, Mr Peters stated that the post on a marketing forum by Mr Rashmi Patel of Bitstacker was undertaken in order to know more about content-locking and who was undertaking this. It was a 'honeypot' approach so that Bitstacker could identify those using content-locking and avoid doing business with them.
28. Mr Peters stated that it was possible for customers to obtain the 5 free lines offered and then unsubscribe from the service without incurring a charge. Indeed, some 20-30% of people did do this and many did claim prizes on this basis without having been charged at any point.

**Documentary evidence considered by the Tribunal**

29. In its initial response to the Emergency Procedure dated 2 July 2013, Bitstacker stated in correspondence that Adscend *"is not a company which is known to us or that we have any direct or indirect commercial relationship with"*.
30. In response to a request from Mr Lewis to cease the promotion of its service, Adscend responded by email on 8 July 2013 to state: *"Hi Mark, thanks for reaching out. I can confirm that your LottoByText offer was paused last week immediately upon request."*
31. In an email dated 10 July 2013 sent to the Executive, Adscend stated as follows in relation to the ransomware issue raised:

*"We are taking this matter as seriously as PhonepayPlus and investigating the source involved with this form of promotion, known as "ransomware". This is not an acceptable form of promotion allowed by us, any of our partners, or anyone in the affiliate marketing industry.*

[Reference was made to the terms and conditions and advertising guidelines which Adscend required its publishers to adhere to.]

*In addition, we have a compliance specialist that proactively looks for violations of our terms, guidelines, or any applicable laws/policies.*

*As you are familiar with as a mobile pin submit regulator, I'm sure you are familiar with rogue companies that exist, operating outside of your guidelines, and abuse services.*

*To clarify on this matter, we are a performance-based network that works with hundreds of active publishers at any given point. In this instance, it has been discovered that the "ransomware" was not done directly via our network, rather we work with a large publisher that has its own set of affiliates/publishers. Upon identification of the ransomware issue, we contacted them promptly and had the issue taken care of. This issue has been isolated to just them on our network. They hold their publishers to the same standards as we do – and the violation was taken seriously and the publisher was banned with payment withheld from the network. I believe notice was also posted by the publisher to their subaffiliates/publishers warning against this type of promotion.*

*Unfortunately, given the issue routed through one of our partners rather than directly through us, this is the scope of assistance we can personally provide. However, if it would be helpful, we can introduce you to the third party publisher for you to carry a further conversation."*

32. Following this email, the Executive asked to be introduced to the third party publisher. Adscend responded by email, copying in *"the third party network that dealt with the rogue "ransomware" publisher. They will be able to provide you with more information in regards to the rogue publisher you are looking for information for."* In the event, the Executive did not make contact with this third party network.
  
33. Bitstacker produced a further email from Adscend dated 23 July 2013 which stated: *"As confirmed, we do not see any leads in our system related to the rogue sub source. Our publisher has thousands of sub publishers under them, so while its possible leads came through*



*your offers from that top tier publisher's ID via their other sub publishers, it does not confirm they came from the one rogue sub source that was identified".*

34. A further email from Bitstacker dated 26 July 2013 was also produced which stated *"We do not have a contract in place with you, however as confirmed, we do not see any leads in our system for LottoByText, related to the rogue sub source identified"*.

#### **Submissions of the parties**

35. The Executive accepted that if the activities related to the wifihackpassword website and associated ransomware were the acts of parties with no direct or indirect connection with Bitstacker, then Bitstacker did not bear responsibility for their actions. But the Executive contended that if acts were carried out by a party with some commercial arrangement with Bitstacker or one of its affiliates, even if there were a number of parties interposed in-between Bitstacker and the rogues, then Bitstacker was responsible for their breaches of the Code.
36. The Executive referred to Part 2 of the Code (on page 5), which states *"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"*. By contrast, in the same paragraph it is stated that Network operators and Level 1 providers *"must take all reasonable steps in the context of their roles to ensure the rules are complied with"*. The Executive also referred to a Compliance Update published on 16 February 2013 entitled *"Misleading digital marketing of premium rate services"*. This guidance stated that the Code did not directly govern the activities of affiliate marketers and that *"responsibility for the actions of affiliate marketers remains with the relevant PRS provider. If PRS providers contract, or enter into arrangements, with affiliate marketers who then act in breach of the Code when promoting their services, the PRS provider can expect to be held responsible by PhonepayPlus for the relevant breach."*
37. The Executive contended that the evidence demonstrated that the link on the wifihackpassword website redirected traffic via Adscend to the lottobytext website. Even if there was not a direct contractual link between them, Adscend was clearly a sub-affiliate of Bitstacker. Accordingly, the redirection would potentially have triggered a payment which would have cascaded down to the rogue responsible for the wifihackpassword site. The malware was thus a malicious and deceiving form of promotion which was operated in the

hope of directing traffic to the lottobytext website (among others) and thus triggering some financial gain. Given the relevant regulatory framework, it was proportionate and in accordance with the Code for Bitstacker to be held responsible for this promotional material.

38. The Executive also asserted that the phrase “*the smart way to play the National Lottery*” was misleading. It pointed out that the lottobytext service offers less good value for money than buying lottery tickets directly.
39. The Executive also contended that the offer “*Get 5 Free Euromillions/Lotto Lines on your mobile*” was misleading. This was said to be because consumers were only offered the free lines as part of a syndicate, and they had to subscribe to the service in order to obtain the free lines.
40. Bitstacker challenged the Executive’s case as to the malware in two central respects. First of all, Bitstacker contended that the evidence did not demonstrate that the purpose of the wifihackpassword website was to divert traffic to certain websites in the hope of triggering payments. Bitstacker relied in particular upon the contention that the link in question was derived from an internal email campaign and could not have been monetised. Bitstacker pointed to the alternative possibility that the malware was intended to capture the personal information that would have had to have been entered when registering on the lottobytext website.
41. Secondly, even if there were some commercial link between Bitstacker’s marketing affiliates and those who deployed the malware, Bitstacker contended that it would be disproportionate and counter to legal principle for Bitstacker to be held responsible for the activities of third parties in this way. Bitstacker relied upon a number of European and English authorities in support of this proposition.
42. Bitstacker did not dispute that holding a Level 2 provider responsible for the activities of those with whom it directly contracted (as referred to in the Compliance Update cited above) was a proportionate approach. But Bitstacker argued that the position was different if a sub-affiliate marketer (or indeed a party at even greater contractual distance from the Level 2 provider) was appointed of whom the Level 2 provider knew nothing. In circumstances where such an appointment was not authorised by the Level 2 provider, and where the activities of the sub-

affiliate were not under its control, it would be disproportionate to hold the Level 2 provider accountable. Bitstacker contended that the most that could be expected of them would be to hold them responsible for those parties whom they knew and directly contracted with.

43. Bitstacker argued that it did not expect its marketing affiliates to go out and place the marketing work with others, but it was accepted that there was no explicit prohibition on the use of sub-affiliates in its contracts. Bitstacker also accepted that it was industry practice and an industry expectation that marketing affiliates would use sub-affiliates.
44. In relation to the content of the lottobytext website, Bitstacker argued that the phrase "*the smart way to play the National Lottery*" was in fact justified by the services which Bitstacker provided. The lottobytext service allowed consumers to join a syndicate, and thus increase their chances of a win, without having to deal with the practical and legal obstacles which would otherwise exist. The fact that the winnings would then have to be divided between the members of the syndicate did not mean that this phrase was misleading.
45. In relation to the advertising of "*five free lines*", Bitstacker contended that this was factually accurate. Consumers could indeed enjoy five free lines and then cancel their subscription without paying any charge.

## **Discussion**

### Use of malware: factual issue

46. The primary factual issue between the parties was whether there was any commercial link between the malware deployed by means of the wifihackpassword website and the lottobytext website. It was common ground that Bitstacker could not be held responsible for the activities of the third party propagator of the ransomware unless it was the case that the link to Bitstacker's website used by it could potentially result in a payment being triggered which would cascade down to the rogue. If the link did not potentially trigger such a payment, then on any view the malware could not be deemed to be a promotion of Bitstacker's service.
47. The Tribunal must decide this issue on the balance of probabilities. It should be said at the outset that the evidence on this issue was not as full or comprehensive as it might have been. However, the four following pieces of evidence in particular were important:

- 47.1. Mr Lachhani's evidence that he saw the URLs for Adscendmedia.com and Filefire.org flash up in the brief interstitial moment as the consumer was redirected to the lottobytext website. If correct, this evidence is not consistent with the link having been derived from an internal email campaign, and it points to the kind of arrangements which would allow Adscend to trace the source of the redirect in order to allocate any payment triggered appropriately;
- 47.2. The evidence from Adscend. The email of 10 July 2013 to the Executive was relatively detailed and clear, and appeared to show that Adscend had traced the malware to an affiliate of a large publisher which it worked with. Thus the rogue affiliate was not among Adscend's own network of affiliates, but was linked to a third party publisher with whom Adscend had a commercial arrangement. Adscend's correspondence indicated that it had the ability to identify the source of the claim for payment for the promotional activity and to block payment where the affiliate had behaved unacceptably. Further emails from Adscend produced by Bitstacker provided a somewhat vaguer picture (as set out above);
- 47.3. Bitstacker's evidence that the link producing the redirect to the lottobytext website came from one of its own promotional email campaigns. This was a crucial piece of evidence which will be considered further below;
- 47.4. The possibility that the malware was intended to capture personal information rather than direct traffic to websites in the hope of triggering payments.
48. On balance, and after having carefully considered all the relevant evidence on this issue, the Tribunal was satisfied on the balance of probabilities that the link to the lottobytext website associated with the malware was included with the intention of redirecting traffic and collecting the resulting payments triggered. The Tribunal accepts Mr Lachhani's evidence that he saw the URLs for Adscendmedia.com and Filefire.org flashing up in the brief moment as the page redirected. Mr Lachhani came across as a careful and convincing witness, and he made a contemporary note of the web addresses which he saw. This evidence points strongly towards there being a commercial link (through an unknown number of intervening third parties including Adscend) between Bitstacker and the rogue.
49. The account given by Adscend in the email of 10 July also clearly supports this version of events. It is hard to believe that Adscend would have written this email if their investigation had revealed that the link between the malware and the lottobytext website had not been

facilitated by their system at all. One would expect this to have been the first point which they would have made to a regulator in these circumstances, but rather they set out their positive findings that the link had been traced and positively identified. The offending publisher was banned and payments were withheld. The email of 10 July does not make any sense in the alternative factual scenario where the link to the lottobytext website was an internally generated Bitstacker link not involving Adscend or its affiliates and publishers at all.

50. It is true that the evidence from Adscend is not comprehensive or entirely consistent. The further emails from Adscend produced by Bitstacker are less clear than the fuller account given on 10 July. These emails are brief, but they do to some extent detract from the clear picture which the email of 10 July appears to give. It is a pity that neither the Executive nor Bitstacker contacted Adscend to obtain a final and definitive account. The Executive also did not contact the third party publisher as they were invited to do by Adscend to obtain further corroborating evidence. Nevertheless, the Tribunal considers that overall the evidence from Adscend supports Mr Lachhani's contention that the redirect went via Adscend's system.
51. Bitstacker denied having any contemporary knowledge of Adscend's activities on its behalf. But the evidence adduced by the Executive clearly demonstrates that Adscend was a regular referrer of traffic to the lottobytext website. Mr Lewis accepted in evidence that this link was present.
52. The Tribunal considered carefully Bitstacker's contention that the link to the lottobytext website was derived from one of its own internal email campaigns. However, the evidence in support of this contention was unsatisfactory. Mr Lewis could not provide any documentary evidence demonstrating that this was the case. The raw data which was apparently interrogated in order to trace the provenance of the link in question was not retained, and the Tribunal find this very surprising in the context of the Emergency Procedure instigated by the Executive. In the circumstances, the Tribunal was unable to put much weight on Bitstacker's assertion.
53. It is true of course that Mr Lachhani also did not produce any documentary evidence demonstrating that the link redirected via Adscendmedia.com. However, this was because he was unable for practical reasons to capture the relevant URL in a screenshot. He did make a contemporary note which he produced in evidence. Bitstacker's failure to produce the

available evidence which would have substantiated its contrary assertion weighed against it in the Tribunal's assessment.

54. Bitstacker's alternative explanation for the malware was that it was intended to capture personal data. The report which Bitstacker relied upon in support of this possibility was not of great assistance to the Tribunal and did not include any detailed analysis or consideration of the particular software in question. There was no persuasive evidence to support Bitstacker's theory, and the Tribunal was not satisfied that data capture was likely to be the underlying purpose of the malware.
55. Bitstacker made the point that the use of such malicious content-blocking software would not result in the consumers who arrived at lottobytext's website being likely to subscribe to the service for the necessary period of time which would result in any benefit to them. This may well be the case. But the propagators of the malware included links to various different websites in the hope of triggering payments. It would be unsurprising if these individuals failed to study the underlying business of the relevant service providers and simply adopted a scatter-gun approach, co-opting various links obtained from affiliate marketers in the hope of triggering payments. In the Tribunal's view, the fact that any such payment may, in the case of Bitstacker's service, have been unlikely to materialise does not stop the malware from being a promotion of the service for the purposes of the Code.
56. The Tribunal do not consider that the posts made by Mr Patel on the internet marketing forum are of any assistance to it on this issue.
57. In conclusion, the Tribunal finds that there was some commercial arrangement, probably of significant complexity, linking Bitstacker and the rogue propagator of the malware. The Tribunal thus does find that the intention of using the link was to direct traffic to the lottobytext website in the hope of triggering a payment. Thus the malware was a 'promotion' of Bitstacker's service for the purposes of the Code.

#### Use of malware: legal issue

58. The Tribunal accepts as uncontroversial the central proposition relied on by Mr Beal on behalf of Bitstacker that PhonepayPlus as a regulator must act in accordance with the principle of

proportionality. Proportionality is a central tenet of good regulation, and one which governs all of PhonepayPlus' regulatory activities.

59. The Tribunal also accepts the general proposition that holding a regulated party responsible for the actions of a third party requires some justification. As Bitstacker accepted, this does not mean that punishing one party for the misdeeds of another is never justified, but regulators need to ensure that such responsibility for third parties is justified by the regulatory context and is limited to what is proportionate to the regulatory aim which is sought to be achieved.
60. However, the Tribunal does consider that in the relevant regulatory context in which the Code is produced, it is proportionate and reasonable to hold Level 2 providers accountable for the activities of those to whom they delegate their marketing activities. As was common ground at the hearing, in the case of online affiliate marketing the delegation of marketing activities to third parties is common and industry-wide. Such activities are then delegated and re-delegated in turn to networks of sub-affiliates and publishers. There may be many parties in the value chain between the regulated Level 2 provider and the individual who is in fact producing and publishing the promotional material. Tracing and identifying the various links between offending promotional content and the Level 2 provider may not be practicable for the regulator, and should not be a requirement for the application of the Code. For regulation to be effective the important obligations set out in the Code must be enforceable against regulated entities otherwise consumer protection will be detrimentally affected.
61. Bitstacker accepts that such an approach is justified where the relevant promotion is effected by a party with whom a Level 2 provider contracts directly, but suggests that the position should be different when the activities are further delegated to sub-affiliates or those with an even more indirect commercial link to the Level 2 provider. The Tribunal does not agree that this is a sensible or coherent distinction. The result would be that regulatory oversight is rendered toothless by the simple means of keeping those responsible for promotional activities at at least two contractual removes.
62. The Tribunal also does not accept that it is unreasonable or unfair to hold Level 2 providers accountable for the activities carried out on their behalf. Bitstacker complained that it was unreasonable to hold it accountable for the acts of those whom it did not have direct

knowledge of, and that no further steps could reasonably be expected of them. The Tribunal disagrees. The Tribunal would have expected Bitstacker to have had some knowledge of Adscend's activities on its behalf, in circumstances where Adscend diverted a large volume of traffic to the lottobytext website. The fact that Bitstacker's evidence was that it was entirely unaware of Adscend's role until contacted by the Executive suggests that Bitstacker took no direct interest in who was promoting its service or how, and that it operated with very little knowledge of the marketing activities carried out on its behalf. Bitstacker cannot rely upon the fact that the promotional activities had been delegated to others as resulting in a dilution of its responsibilities, when such delegation is entirely standard practice in the industry and was envisaged by the terms of the contracts which Bitstacker entered into.

63. Bitstacker authorised the promotion of its service by contracted affiliates, and allowed these affiliates to delegate promotional activity to a network of further affiliates (who were not known to Bitstacker), and who gained an ability to claim indirect payment from Bitstacker for arranging promotional activity on its behalf. The particular activities undertaken by any affiliate, including the operator of the wifihackpassword website, were not authorised in advance by Bitstacker. This was Bitstacker's choice. It does not mean that it would be disproportionate to hold Bitstacker responsible for the promotional activities carried out as a result of that choice.
64. As well as appropriate due diligence into those with whom it contracts directly, it would be open to a Level 2 provider such as Bitstacker to insist upon contractual terms with its affiliates which would go a long way to protecting the Level 2 provider against any breach of the Code and to promoting Code compliance generally.
65. For these reasons, the Tribunal does not accept that it is disproportionate or unreasonable for Bitstacker to be responsible for the contents of any promotion of its service carried out by a third party.
66. In any event, as the Executive point out, the Code is clearly predicated on the basis that Level 2 providers will be responsible for compliance in respect of their services, and the Code has been expressly approved by Ofcom as containing provisions which comply with the need for proportionality. In contrast with the obligations of network operators and Level 1 providers, the obligations on Level 2 providers are not qualified in the Code by a requirement only to



take reasonable steps. The distinction here is that those further down the value chain from Level 1 providers are themselves regulated by the Code, and effective regulation does not require that Level 1 providers are held accountable for breaches of the Code by others. By contrast, those with whom Level 2 providers contract with are not themselves regulated by the Code, and the Code requirements must thus take effect against the Level 2 provider for the regulatory aims to be secured.

67. For these reasons, the Tribunal considers that Bitstacker is accountable for the breaches of the Code resulting from the use of the malware. There is no dispute between the parties that the relevant malware, if it constituted promotional material for which Bitstacker was responsible, was unfair for the purposes of paragraph 2.3.1 of the Code, was misleading for the purposes of paragraph 2.3.2, and was likely to induce an unreasonable sense of fear, anxiety, distress and/or offence in consumers for the purposes of paragraph 2.55. These provisions apply as much to the promotion of a service as to the contents of the service itself under paragraph 2 of the Code on p.5.

'The smart way to play the National Lottery'

68. The Tribunal do not consider that the Executive's case is made out in relation to this alleged breach. It is true that using Bitstacker's service might be considered less good 'value for money' in a narrowly mathematical sense, because the amount spent on lottery tickets will lead to lower rewards over time than if the consumer purchased the tickets direct. However, Bitstacker points out that its service enables consumers to join a syndicate without the practical difficulties which would otherwise be involved. Being a member of such a syndicate would drastically increase the prospects of the consumer winning a big prize, even if this prize then had to be distributed among the members of the syndicate.
69. The Tribunal considers that Bitstacker's service did offer extra value to the consumer beyond the mere purchase of lottery tickets. So long as the cost of the services was made clear to the consumer, the Tribunal considers that it is a matter for the consumer to assess whether it is a service which he or she wishes to make use of.
70. As such, the phrase *'the smart way to play the National Lottery'*, in the Tribunal's assessment and on balance, falls within the bounds of advertising puffery and is likely to be understood as such. The Tribunal considers it unlikely that a reasonable consumer would interpret this

phrase as a representation that the return from lottery tickets purchased through Bitstacker would be better than from tickets bought direct.

71. Accordingly, the promotion was not misleading and breach of paragraph 2.3.2 of the Code is not made out.

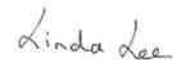
#### 'Five free lines'

72. Bitstacker contended that this offer was factually accurate. Its witnesses stated in evidence that consumers could enjoy five free lines and then cancel the subscription to the service without incurring any charge. Indeed, they stated that many consumers do do this.
73. The Executive did not produce any compelling evidence contradicting the account of Bitstacker's witnesses and the Tribunal accepts this account. Accordingly, no breach of paragraph 2.3.2 of the Code is made out in this respect.

#### **Sanctions**

74. The Tribunal considers the breaches of the Code in relation to the use of the ransomware to be very serious. The propagators of the malware acted illegally and maliciously, with the deliberate intent to deceive and inconvenience individuals for monetary gain. Although only a very limited number of people appear to have clicked on the link to the lottobytext website promoted by the malware, there was the clear potential for a significant detrimental impact on consumers. The use of such malware was likely seriously to damage consumer confidence in premium rate services. Although Bitstacker did not itself disseminate the malware, it must be held responsible for its use under the Code and the seriousness of the use of malware must therefore impact upon the relevant sanction to be imposed.
75. In terms of aggravating and mitigating factors, the Tribunal notes that there were some efforts made by Bitstacker to carry out due diligence in relation to those it contracted with. However, these efforts do not constitute mitigation in circumstances where it appear to have taken no steps in relation to sub-affiliates and those further down the value chain. The fact that it was apparently entirely unaware of Adscend's central role in the marketing of the lottobytext website does not shed a favourable light on Bitstacker's concern as to what was being done on its behalf. On balance, the Tribunal does not consider that that Bitstacker's due diligence activities amount to significant mitigation in these circumstances.

76. The Tribunal takes into account the detriment already suffered by Bitstacker as a result of the use of the Emergency procedure.
77. In all the circumstances, the Tribunal considers that the appropriate sanctions to be imposed are a formal reprimand and a fine of £25,000. Bitstacker should be aware that if it fails to ensure that measures are in place to prevent such harm in the future, it should expect a more significant penalty for a similar breach.
78. The vast majority of the costs incurred by the Executive related to the allegations relating to the malware. Nevertheless, the Tribunal does consider that Bitstacker's limited success in relation to the two subsidiary allegations made should be reflected in the administrative charge paid, and accordingly it also recommends that Bitstacker should pay 90% of the administrative charge under section 4.10 of the Code.



**Linda Lee**

(Chair of the Oral Hearing Tribunal)

Dated this 17th day of March 2014