

Tribunal meeting number: 246

Case reference: 134234

Type of service: Multi-media subscription service

Level 2 provider: Net Real Solutions SL (Spain)

Network operator: all network operators

This case was brought against the Level 2 provider under Paragraph 2.3.3 and Paragraph 2.3.2 of the 14th Edition of the Code of Practice.

The identities of some third parties referenced in this adjudication have been anonymised.

Background and investigation

The Level 2 provider for the Service was Net Real Solutions SL (the “**Level 2 provider**”, the “**NRS GROUP**”). The Level 2 provider was first registered with the Phone-paid Services Authority (the “**PSA**”) on 8 January 2015. The Level 2 provider was based in Spain. The Executive sought derogation and received this from the home member state on 27 January 2017.

The service operated via an aggregator for the Service shortcode (“**the Level 1 provider**”).

The case concerned a multi-media subscription service, ‘Applicateka’ (the “**Service**”) operating on shared shortcode 64055 and Payfortit.

The Level 2 provider gave the following description of the service flow:

1. User clicks on the banner



2. User access to the promotion



3. User click to Subscribe button and is redirected to the carrier billing page where accept the terms and conditions



From Appicateka

Subscribe to appicateka until you text STOP to 64055. This charge will be added to your mobile phone

Subscribe Now for £4.50 per week

3 & Payforit terms



From Appicateka

Subscribe to appicateka for £4.50 per week until you text STOP to 64055

Confirm this charge to your mobile

4. User is subscribed



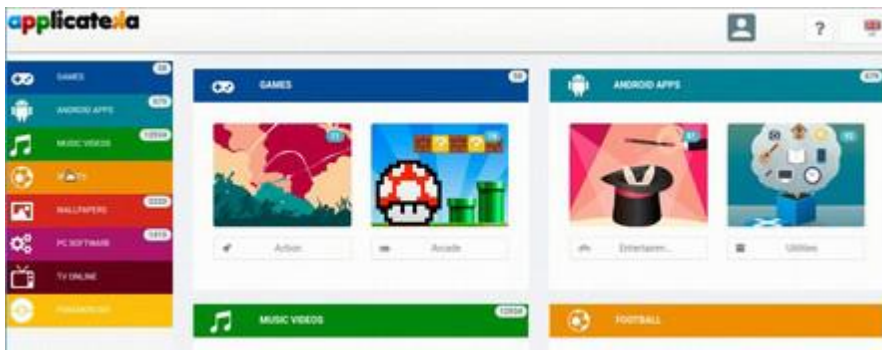
Congratulations! Thanks for joining

You subscribed to Appicateka with the phone number

Register to play

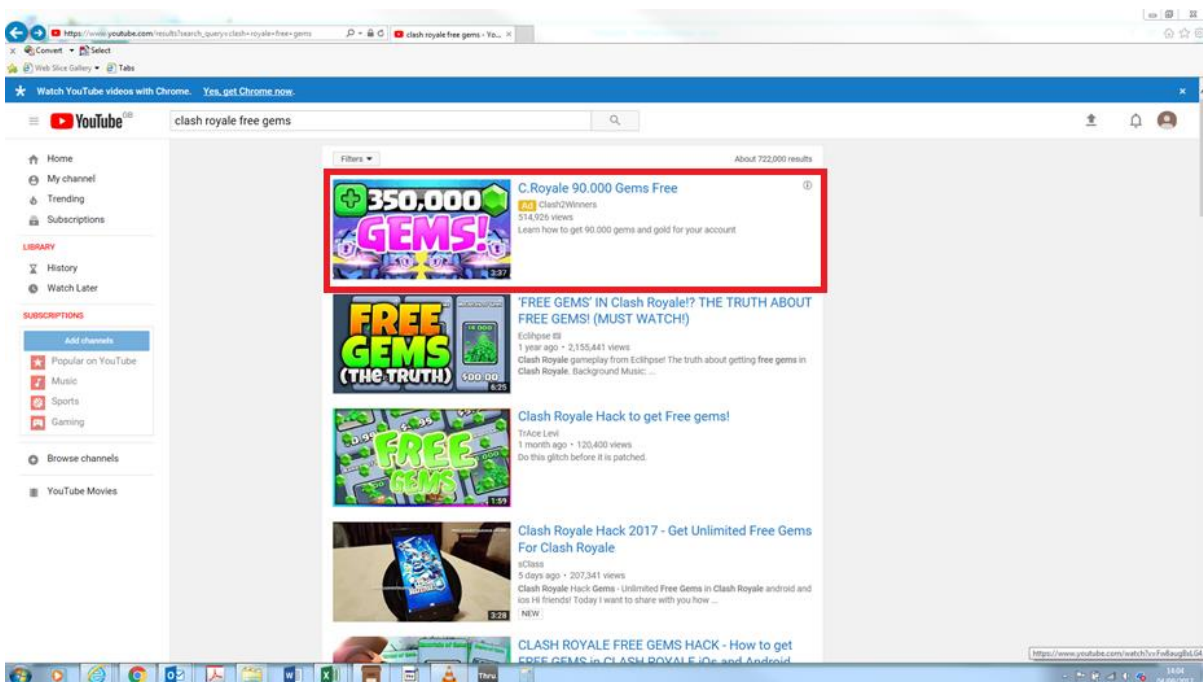
Service for +18 users only. All minors under 18 are not allowed to subscribe or use the service. This is a subscription service costing £4.50 per week until you send STOP to 64055. If you choose to enjoy the content from the service you will enter into the subscription. By signing up for this service you agree that you are 18+ and have the permission of the account holder. You also acknowledge that you have read the [Terms & Conditions](#). For help, please call 020 3129 2986 or contactinfo@nrs-group.com

5. User access to thousands of mobile contents

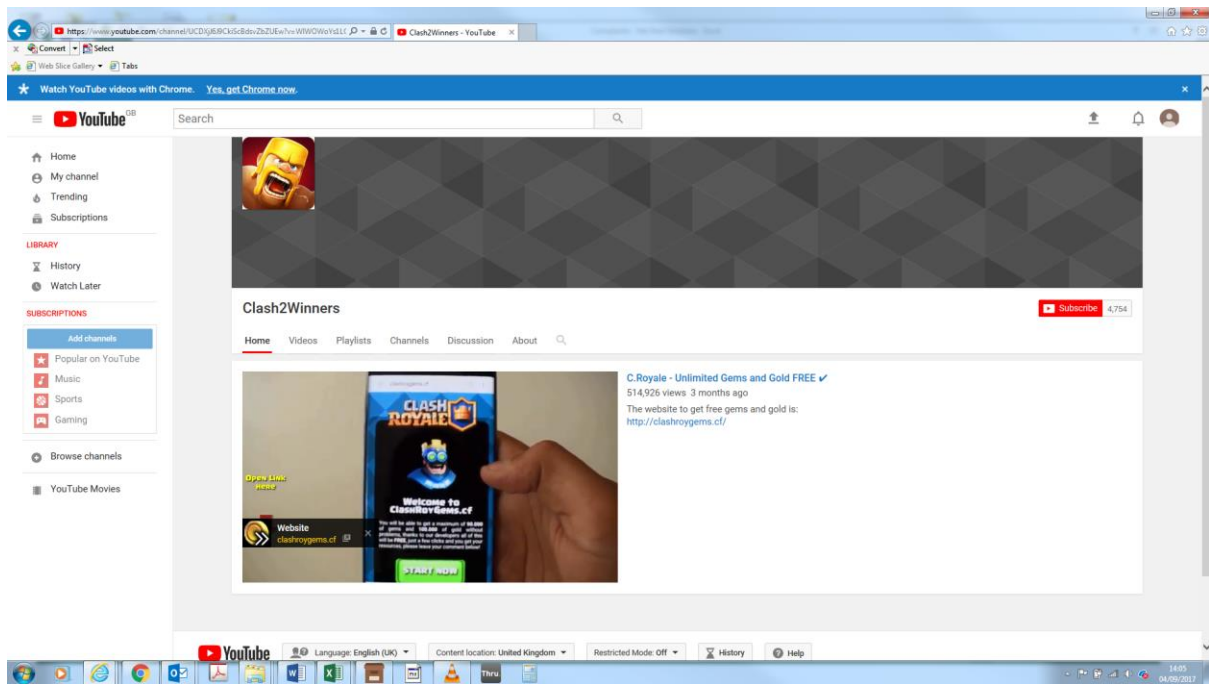


The Executive noted that one of the complainants said that their son had subscribed to the Service on the promise that they would receive free “gems” (virtual currency) for the mobile game Clash Royale. The complainant stated that the promotion was found on the popular video streaming website YouTube. Viewers of the promotional video were asked to visit the website <http://clashroyalgems.cf>.

On 4 September 2017 the Executive found the promotional video on YouTube using the search term “clash royale free gems”. It was noted that the promotion was at the top of the search results as a paid advertisement:



Clicking on the video thumbnail resulted in being taken to a page containing an instructional video on how to obtain free virtual currency by subscribing to the Service for a charge of £4.50:



A copy of the YouTube video was sent as a separate attachment. The Executive tested whether the promise of free virtual currency was true by following the method outlined in the video. The Executive subscribed to the Service as per the video's instructions, but the promised virtual currency was not received

On 2 October 2018, the Level 1 provider, advised the Executive that it had identified a separate issue where consumers had been subscribed to the Service as a result of malware/and or signed up to the Service without their consent. the Level 1 provider provided the following information regarding the malware issue:

"The malware affected the customer's website where by it allowed the merchant to raise a request for a new service, at this point before the page was loaded, the malware intercepted the url to Consent page and change it effectively to create a successful subscription.

By doing this the malware enabled the request to skip the first two pages of the payment flow (call-to-action and confirm-action) and call the create action (this is where the subscription is created) directly."

A sample of complainant accounts have been provided below:

I have not signed up for this service or any other service and don't even know what I am supposed to be getting, but have been being charged 4.50 a week for past 3 months.

consumer said her son attempted to get free "gems" for a game: Clash Royale
 Clash Royale is a gaming app which her 14 yr old son uses
 consumer said her son completed some steps online via <http://clashroyalgems.cf/>

This supplier has somehow tricked me into signing up for a service, which is costing £4,50 last month and this month cost £9.00 . I have not agreed to this service and it is fraudulent

I spontaneously received the message copied above twice, claiming I was subscribed to a service called applicateka, part of the NRS group. I did not sign up to such a service and have since discovered this is a common scam that has affected several people in the past. I was charged £4.50 on three occasions, each separated by a week, and would like to know how I can reclaim this money.

Interim measures in place

On 10 September 2018 the Tribunal imposed a withhold of service revenue of up to £115,000. The Tribunal determinations in respect of the imposition and subsequent review of the interim measures can be found at Annex A.

Apparent breaches of the Code

The Executive believed that the service contravened the Phone-paid Services Authority Code. The malware had the effect of bypassing steps two and three of the user flow as outlined by the Level 2 provider. Specifically, the steps which required a consumer to consent to being charged. The Level 1 provider confirmed that 33,450 consumers had been affected by the malware issue. The Level 1 provider stated that the malware issue affected subscriptions between 1 May and 16 July 2018.

Summary of complaints

The Executive had received 718 complaints concerning the Service since 24 April 2017.

Complainants variously alleged that the Service charges were unsolicited.

of Practice 14th Edition ("the Code") and in particular the following Code provisions:

- Rule 2.3.2 – Misleading
- Rule 2.3.3 – Consent to charge

Alleged breach 1

Rule 2.3.2 of the Code states:

"PRS must not mislead or be likely to mislead in anyway."

1. The Executive stated that the Level 2 provider had breached rule 2.3.2 of the Code as the provider had used content locking as a means of promoting the Service and the promised inducements were not delivered. Content locking is defined in the PSA's Guidance on Digital Marketing as:

"Specifically this relates to marketing techniques used by one party, such as an affiliate marketer, to generate leads and increase conversions for a second party's online service transaction. Consumers are often induced to make the payment on the second party's website because they believe it is the only means of accessing the original party's content, and not because of any interest in the product or service for which they make payment. Furthermore, commission from the payment goes to the marketing affiliate to pay for content that may be presented as being "free".

The Code and Guidance regarding digital marketing makes it clear that it is the responsibility of the Level 2 provider to control affiliate marketing carried out on their behalf:

"1.5 This Guidance also clarifies that it is the responsibility of providers to control affiliate marketing carried out on their behalf and sets out some recommendations as to how to do so safely. For further assistance on controlling risk when using affiliate marketers please read part 10 of the 'Promoting premium rate services' Guidance."

The Executive noted that the Level 2 provider had a history of using content locking as a means of promoting the Service. In response to a direction for information, the Level 1 provider supplied copies of correspondence between it and the Level 2 provider. Contained within this correspondence was an email dated 22 March 2016, whereby the Level 1 provider had warned the Level 2 provider regarding the use of content locking to promote the Service. At this time the Level 2 provider was warned that further use of content locking could lead to a suspension of the Service.

The Executive sent an informal enquiry to the Level 2 provider on 11 May 2017, following monitoring it had conducted of the service. In this correspondence the Executive highlighted its concerns regarding the Service, specifically that consumers may have been misled into opting into the Service based on an incorrect belief that they would obtain virtual currency for games. In its response dated 18 May 2017, the Level 2 provider confirmed the use of content locking to promote the Service. The Level 2 provider supplied details of three promotions where content locking was used to promote the Service.

The Level 2 provider said, *"the damage of the campaigns is very low, we maked 181 conversions"* [sic]. In addition, the Level 2 provider advised that it had identified the affiliate (Affiliate 1 Media LLC) as being responsible for the content locking promotion and cancelled its advertising contract with them. In addition, the Level 2 provider stated:

"From all this issue we have thoroughly reviewed all the other agencies we work with to ensure that no other agency is doing something similar and informing that it is not allowed to do it more in the future."

On 1 June 2017, the Executive received a complaint about the Service. The complainant stated that her son had been encouraged into subscribing to the Service in the belief that he would receive virtual currency for the popular mobile game, Clash Royale:

"consumer said her son attempted to get free "gems" for a game: Clash Royale

*Clash Royale is a gaming app which her 14 yr old son uses
consumer said her son completed some steps online via
<http://clashroygems.cf/>*

*consumer reports misleading promotion she said Clash Royale is an app but she doesn't believe
it has anything to do with this website
an advert that popped up on Youtube - sponsored content"*

The Executive conducted monitoring of the Service on 30 August 2018. The monitoring demonstrated that the promised free gems were not provided upon subscribing to the Service. On 28 September 2017, the Executive sent a formal direction for information to the Level 2 provider. A copy of the monitoring was enclosed. The Level 2 provider advised that Affiliate 2 was responsible for the promotion. The Level 2 provider advised that 763 subscriptions had been initiated as a result of this promotion.

The Level 2 provider had previously advised the Executive that it employed the third-party monitoring house, Empello, to monitor its promotions. The Executive requested copies of the monitoring conducted by Empello. The Executive noted that Empello had found a content locking journey on 22 September 2017. The Level 2 provider stated that it had stopped "*all the offers activity with the Partner*".

The content locking journeys found by the Executive in August 2017 and by Empello in September 2017 indicated that the actions the Level 2 provider stated it had taken in May 2017, namely reviewing its agencies, were not effective. The Executive's view therefore was that the repeated use of content locking by affiliate agencies demonstrated that the Level 2 did not exercise sufficient control and oversight of how the Service was being promoted. Therefore, in spite of the Level 2 provider's assertion that it had reviewed its agencies, its lack of control over the way the Service was promoted led to further harm to consumers.

The Executive tested the content locking journey as outlined in the consumer's complaint above. The complainant had stated that her son had been encouraged into subscribing to the Service in the belief that he would receive virtual currency for the popular mobile game, Clash Royale. This game was free for consumers to download but offered in-game purchases in the form of 'gems', which could be used as in-game currency to purchase addition items/bonuses. The Executive relied upon the screenshot below showing the cost of the gems within the game:



The screenshot showed that gems, in various amounts, could be purchased at different price points with the maximum amount of 14,000 gems costing £99.99. The Executive found the Service promotion on YouTube:



C. Royale 90,000 Gems Free

Ad Clash2Winners • 515K views

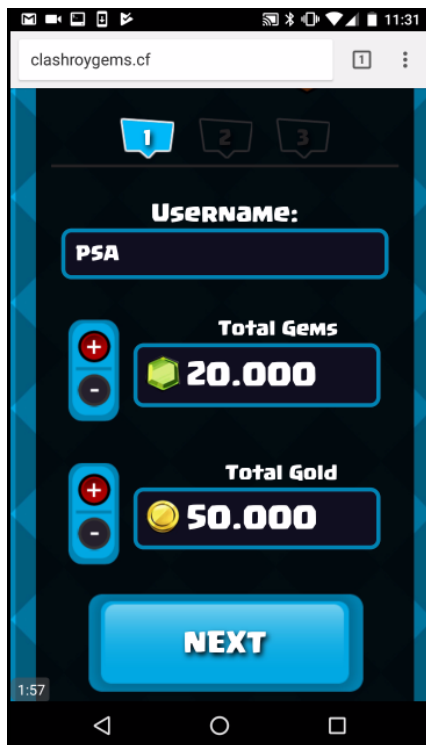
Learn how to get 90,000 gems and gold for your account

The promotion suggested that consumers could obtain "90,000 Gems Free". The equivalent cost of purchasing 90,000 gems within the app would be £689.82. Therefore, this promotion would be attractive to consumers looking to obtain gems for free. At the time of finding the promotion, the video had received 514,926 views.

On 30 August 2017, the Executive had proceeded to test the validity of the of the claim that virtual currency could be obtained by subscribing to the Service. The video instructed consumers to go to the website <http://clashroyalgems.cf>:



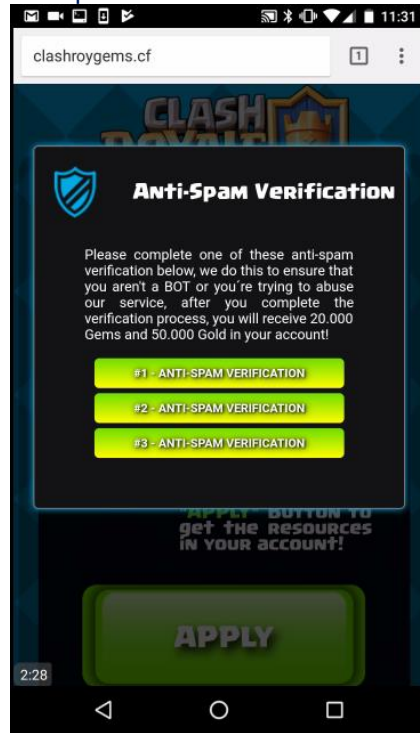
Once on the website, consumers are asked to put in their Clash Royal username and enter the amount of virtual currency they wish to receive:



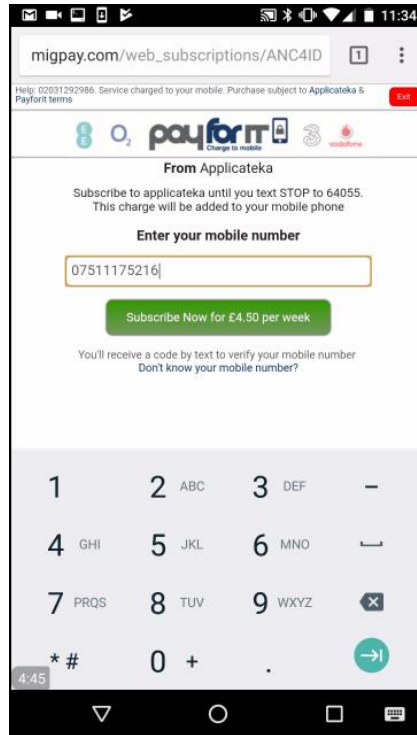
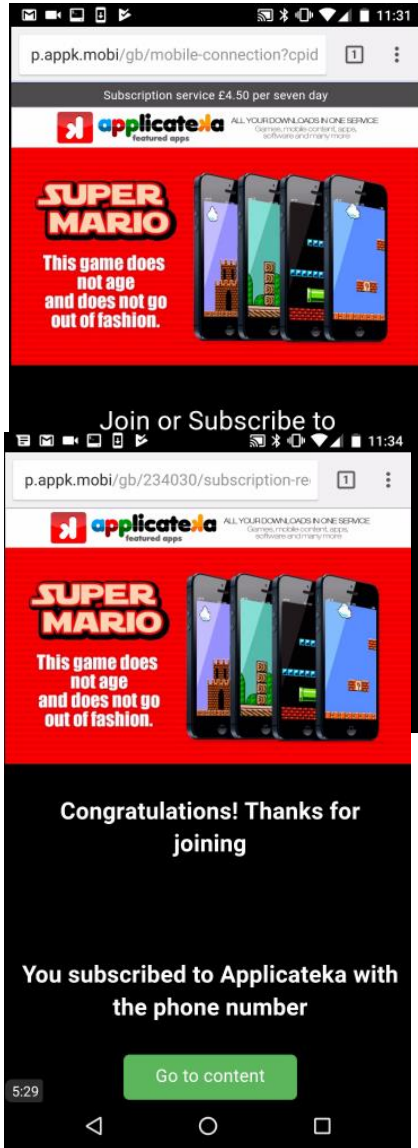
The website purported to process the request:



The consumer is asked to 'Apply' the virtual currency and are taken to a verification screen. The consumer is informed they must compete this verification to receive the virtual currency:



Selecting one of the verification options resulted in being taken to the Level 2 providers landing page. The Executive proceeded to subscribe to the Service:



The Executive checked the Clash Royale application to see if the virtual currency had been applied. A total of 20,000 gems and 50,000 gold had been requested but no virtual currency had been applied to the game account (see screenshot below):



There was no change to the amount of gems and gold.

The Executive asserted that consumers were likely to have been misled into subscribing to the Service by the content locking promotions, as a result of the offered opportunity to obtain virtual currency for the price of a £4.50 subscription to the Service which in real money terms would have cost in the hundreds of pounds,. Given this incentive, consumers were likely to subscribe to the Service. However, once the subscription had been initiated, the promised virtual currency was not forthcoming.

After testing the Clash Royale promotion, the Executive did not receive the virtual currency as promised and therefore asked the Level 2 provider to comment. The Level 2 provider responded:

"We allready informed the Partner that must contact all users suscribed to the campaign and offer them the content promised. [sic]"

The Executive asked the Level 2 provider to supply evidence that virtual currency had been sent to consumers to which the Level 2 provider responded:

"The Partner ensured that they have delivered a pdf file to all the users that suscribed to the Super Mario offer. This data is included in a sort of terms and conditions of the <http://clashroygems.cf> so the user was informed in all moment that suscribing to the Applicateka offer will receive in exchange a content related to the Clash Royale – tricks, tips, resume of the game, takeaways – Strenghts, Weaknesses, Game play brief, Core-Loop, Progression, King Level, Trophies, Cards, Game content, Chest details, Monetization, Social Features, Notification, Summary, etc. (For more details see file attached to email called "Guide Clash Royale") [sic]"

The Executive noted that the Level 2 provider had stated that the affiliate marketer had supplied all users with the pdf file, referred to above, as a substitute for the promised virtual

currency. The Executive further noted that the Level 2 provider had supplied no evidence that it had sent pdf files to all of the affected subscribers. In addition, the Level 2 provider had supplied no details as to how these pdfs were to be delivered to consumers. The Executive noted that, although the Level 2 provider would have possession of the consumer's mobile number as part of the subscription process, this did not appear to be sufficient to enable the affiliate partner to deliver a pdf file. Furthermore, the Executive had not received the guide during its monitoring of the Service and was only supplied with the pdf file when the Level 2 provider supplied it in its response to the Executive's direction for information dated 30 October 2017.

The Executive reviewed the pdf file supplied by the Level 2 provider, which the Level 2 provider described as a guide providing tips and tricks to win the game. However, the Executive submitted that it was, in fact, a free to download 'teardown' document available from the website <http://adriancrook.com/teardownclub>. The website in question described the purpose of a teardown document as follows:

"At all major game developers, product managers regularly produce teardowns. A teardown is an in-depth analysis of a competitor's product, designed to highlight what can be learned. Product managers then pass these teardowns on to their internal development teams to help them make better products."

The Executive stated that this document was not intended for use by consumers who played Clash Royale, but rather it was intended to provide information to developers to assist them in making better/rival products.

The Executive asked the Level 2 provider to explain how the guide was a suitable replacement for the promised virtual currency. The Level 2 provider responded as follows:

"This pdf file help user to understand better the way Clash Royal game works and can give customer ideas to start making great strategies in order to get more rewards and win battles against their opponents. Every detail of the game is very well detailed on the file, every card, trophies, chests, etc. All this reveals how can the file contribute to the player to continue advancing the stages of the game from the bigginig till the end. [sic]"
We consider suitable replacement for the virtual currency because many of the users might be new to play so they might do not know how the game works. With the file in their hands customer can learn very fast tricks and make good strategies to win their oppponent while if they do not have it, customer might not know how to play and win the game at first. We think this is a competitive advantage for the user who have this file in his power in front of those who do not have it." [sic]

The Executive submitted that Clash Royale was a mobile game whereby players collected cards, which could be used to build battle decks and duel other players in real time. Central to being successful at the game was knowing the strengths and weaknesses of each card, knowing how they interacted with other cards and how they fitted within a battle deck. Such information was freely available online and could be found on websites such as 'clashroyale.fandom.com'.

The Executive compared the information contained in the guide supplied by the Level 2 provider with that found on clashroyale.fandom.com.

The Level 2 provider guide contained a section regarding the cards within the game, as shown in the screenshots below:

Cards

Cards are the core of the *Clash Royale* experience



CARDS

Card Types



Troops



Buildings



Spells

- Cards are used to deploy troops, cast spells, and erect buildings on the battlefield
- Cards can be acquired by finding them in chests or buying them with Gold.
- There will be 42 cards available at launch.

Card Rarity



Common



Rare



Epic



© 2016 Adrian Crook & Associates

14

Cards Continued

Cards can be upgraded to grow with the player

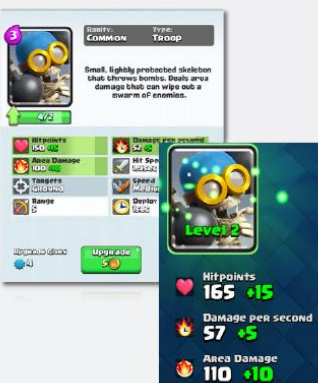
Clash Royale features a card-leveling mechanic that closely resembles fusion mechanics seen in countless other CCGs. This system adds value to collecting multiple copies of cards and acts as a powerful gold sink. With increasing costs per level, *Clash Royale* realizes immense monetization depth for whales.

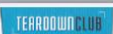
Cards required for upgrade

Level	Common	Rare	Epic
2	2	2	2
3	4	4	4
4	10	10	10
5	20	20	20
6	50	50	50
7	100	100	100
8	200	200	300
9	400	500	--
10	800	1,000	--
11	2,000	--	--
12	5,000	--	--

Gold cost to upgrade

Level	Common	Rare	Epic
2	5	50	400
3	20	150	1,000
4	50	400	2,000
5	150	1,000	4,000
6	400	2,000	8,000
7	1,000	4,000	20,000
8	2,000	8,000	50,000
9	4,000	20,000	--
10	8,000	50,000	--
11	20,000	--	--
12	50,000	--	--



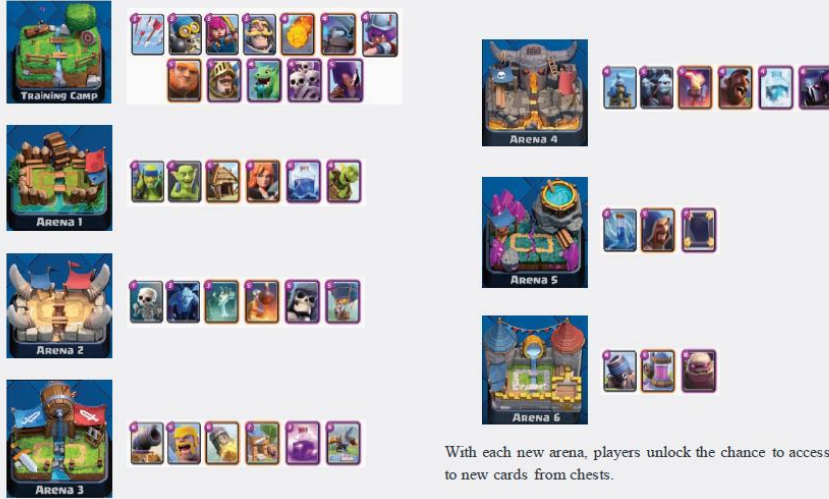


© 2016 Adrian Crook & Associates

15

Cards Continued

Gated access to powerful cards



With each new arena, players unlock the chance to access to new cards from chests.



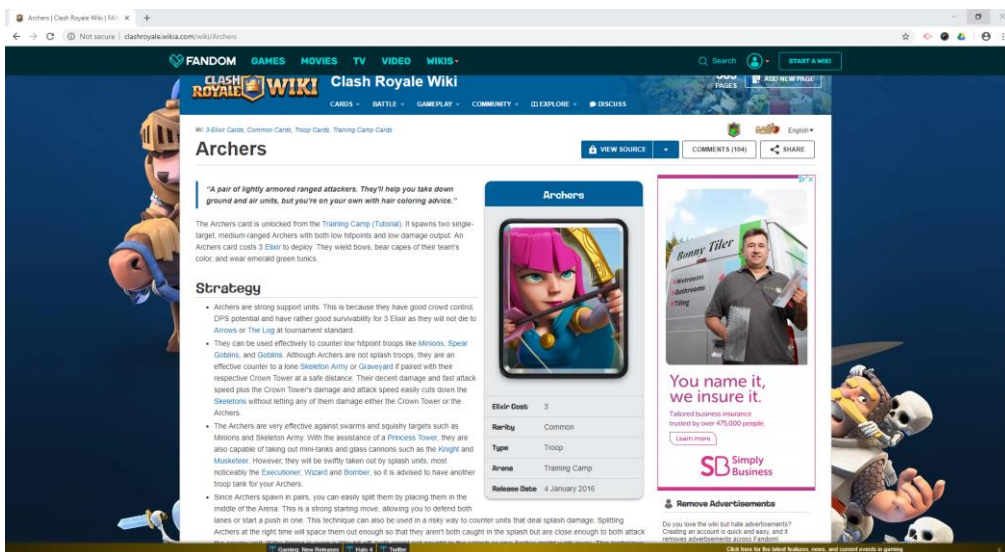
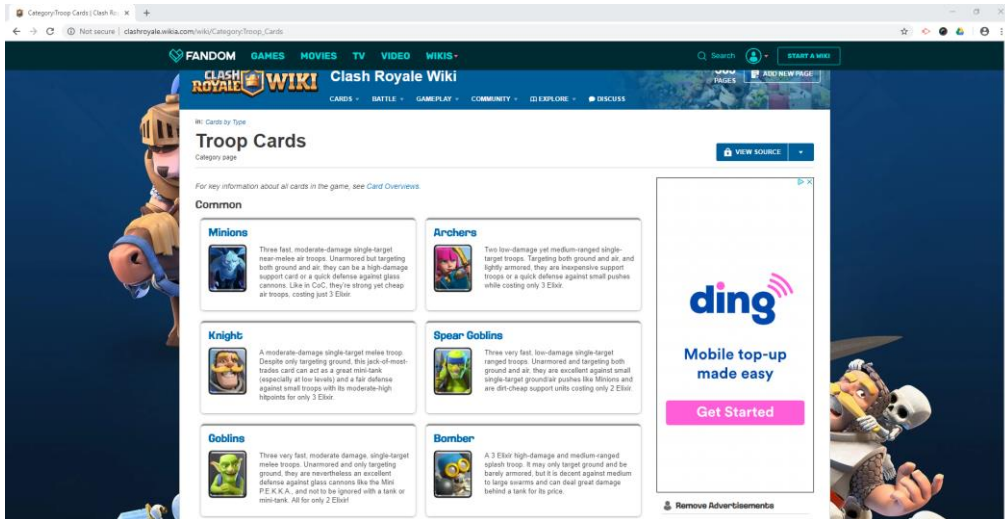
© 2016 Adrian Crook & Associates

16

The Executive noted that the above was a high-level overview of the function of cards within the game, outlining the monetisation opportunities that they presented to game developers, but that it provided no detail regarding the specifics of each individual card or how they could be used in a way that would benefit a player of the game.

In comparison, clashroyale.fandom.com provided an overview of each card and provided a breakdown of the how they could be utilised, as shown in the screenshots below:





The Executive stated that, given that the cards were at the core of the game's mechanic, the guide supplied by the Level 2 provider would be of little benefit to a consumer wishing to learn how to play the game.

The Executive noted that it had not received the pdf guide when monitoring the service but in any event, even if the pdf file had been submitted to all users of the Service, the Executive's view was that the pdf file was not a reasonable substitution for the promised virtual currency as the guide the Level 2 provider supplied did not contain information that would benefit new/and or existing players. It was therefore the Executive's view that guides that were freely available online would be of greater value to consumers. As such, consumers who received the guide as a substitute for virtual currency were not being treated fairly or equitably, having been misled into subscribing to the Service.

It was submitted by the Executive that there was a history of the Service being promoted through the use of content locking and, based on the Executive's monitoring, the advertised incentives were not delivered.

Accordingly, the Executive submitted that the promotional method used to promote the Service was misleading and that the Level 2 provider had breached rule 2.3.2 of the Code.

In response to questioning by the Tribunal the Executive confirmed that it had sought derogation from the relevant authority in the Level 2 provider's home member state of Spain before taking its own measures in respect of the service, in accordance with the requirements of the E-Commerce Directive. The Executive explained that it had outlined its concerns about the service to the Spanish authority who had responded by stating that it did not intend to take its own measures. At this stage the Executive had proceeded to take its own measures.

The Executive also clarified that this was the second investigation into the service and that, since 2016, there had been other incidences of the use of content locking in the marketing of the service, which the Level 2 provider had accepted. The monitoring house, Empello, had found a content locking journey and the service had previously been issued with warnings known as "yellow cards" by the mobile networks as a result of the use of content locking by marketing affiliates. The Executive stated that this matter was therefore not an isolated incident and the issue was not limited to just one advertising partner.

The Executive reiterated that, even where affiliate marketers engaged in the use of content locking, it remained the responsibility of the Level 2 provider at all times to ensure that its service was marketed compliantly, which was made clear in the PSA's Guidance on Promoting Premium Rate Services.

The Executive clarified that, although it had asked for revenue for the service to be taken into account from December 2016 onwards for sanctioning purposes, this was an error and it was in fact revenue generated from January 2017 onwards that should be taken into account. The Executive also confirmed that the revenue it considered to be relevant for sanctioning purposes was the gross Level 2 provider revenue and that any business costs or expenses to the Level 2 provider, other than refunds issued to consumers, were not taken into account by the Executive when assessing the relevant revenue figure for sanctioning purposes.

2. The Level 2 provider denied the breach and its legal representative submitted the following written representations on its behalf:

The Executive asserts that NRS GROUP has breached rule 2.3.2 of the Code on the basis that NRS GROUP itself used content locking as a means of promoting the Service and promised some inducement which were never delivered.

Applicateka and NRS GROUP service

Applicateka is a service owned and provided by NRS GROUP. Applicateka is a service for smartphones but also it is compatible with tablets and PCs. It gives users direct access to thousands of contents for mobile phone like games, videos, wallpapers for WhatsApp, utilities and premium downloads.

NRS GROUP offers through Appicataka services and downloads of entertainment content through its WEB, WAP and SMS services for compatible mobile phones, tablets and/or PC. Appicataka users must be resident in the United Kingdom and must be at least 18 years old or have the bill payers' permission to use the Service.

NRS GROUP with the purpose of promoting Appicataka in United Kingdom cooperates with agencies to carry out advertising campaigns and capture new users offering them landings and banners. With all the agencies with which NRS GROUP cooperates, they sign very solid agency agreements which includes binding terms and conditions that govern the relation between the parties and are legally enforceable. Thus, agreements must be fulfilled by all parties. Furthermore, NRS GROUP establishes in all cases guidelines on how to carry out the promotions in accordance with the English law and the Code.

It should be noted that NRS GROUP recruitment policy consists on working only with trusted advertising agencies that accept the restrictions established and the instructions given. Agencies must sign the agreement that NRS GROUP enables for them. Likewise, once the advertising campaigns are carried out, NRS GROUP is constantly monitoring the campaigns, paralyzing them if at any moment detects any anomaly fact in relation with the signed agreement, the English law or the Code.

Use of content locking

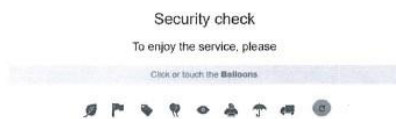
The affirmation the PSA does in the Warning Notice that the provider **(NRS GROUP) used content locking as a mean of promoting the Service is completely false and should not be taken for correct and definite** as NRS GROUP never asked nor indicate any agency to employ said techniques to promote the Service. Furthermore, NRS GROUP always prohibited and banned said techniques and required and obliged the agencies to be compliant not only with the English advertising law but also with the Code.

Content locking, according to the Digital Marketing and promotions Guide is a "*marketing technique used by one party, such as an affiliate marketer, to generate leads and increase conversions for a second party's service transaction*". The Guidance clarifies, in its paragraph 1.5, that it is **the responsibility of the providers** (in our case, NRS GROUP) **to control the affiliate marketing carried out on their behalf and sets out some recommendations as to how to do so safely.**

In the numerous responses that NRS GROUP has sent it is proven that NRS GROUP not only **has controlled its affiliates through its internal protocols** (as explained in our last response dated December 20th, 2018 available at Annex 3, Page 386), but **also has always set out recommendations to do the marketing safely.**

With the aim of optimizing the traffic sources as much as possible and control and monitor the notification of possible late-night /bot registrations that could happen, NRS continuously reviewed the user's registrations reports provided by the affiliates of Xito Media in order to avoid any malware or fraudulent traffic. Also, NRS GROUP constantly reviewed the use of the creations and materials provided to Xito Media in order to comply with the guidelines, restrictions and obligations agreed in the Advertising Agreement.

In addition to all the above, NRS GROUP activated captcha filters in all the URLs of Xito Media as shown in the image enclosed to the Response below.



The aforementioned measures constitute the internal protocol of NRS GROUP (hereinafter, the "Internal Protocol").

Fig. 1: Extract of our response dated December 20th, 2018

- These **recommendations and obligations were indeed exposed in their agency agreements and in the various communications** that took place between NRS GROUP and all the. The communications were formal and informal and even through the fastest means available (for instance, Skype) where NRS GROUP made completely clear that it was (and always be) against the content locking because it is against NRS GROUP's interest and harms the customers and the business in the long term.

Restrictions:

- No incent traffic.
- No content locking
- Don't use banners not reviewed by the advertiser first.
- Don't use misleading advertising.
- No social traffic.
- No redirects.

Find attached the banners.

Fig. 2: Example of an extract of a communication regarding campaigns in UK. (Annex 3 page 197)

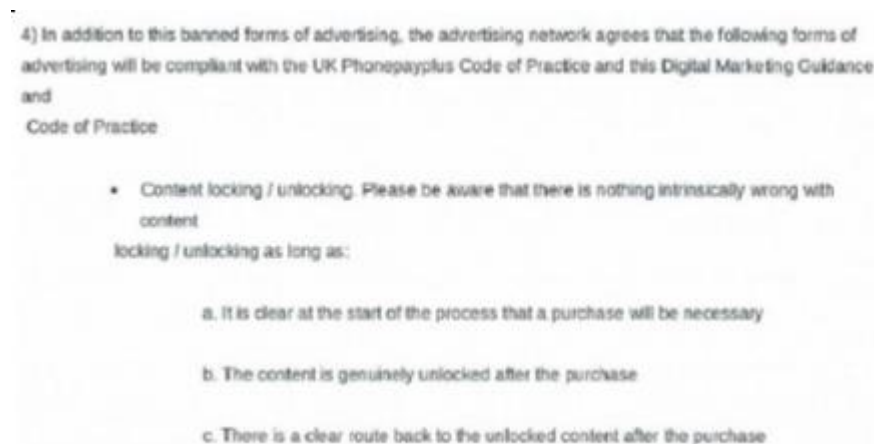


Fig. 3: Clause of an agreement between NRS GROUP and an Agency. (Annex 3, page 201)

These communications and obligations that NRS GROUP has always enforced to the agencies, do nothing else but prove that NRS GROUP has conducted a diligent relation with its agencies requiring them an exquisite fulfilment of the agreement, the English advertising law, the Code and the applicable Guidance.

Every campaign was accompanied by a series of obligations and restrictions that agencies had to take in force not only to be compliant with the English law but also for the own benefit of the consumers. As advocated by NRS GROUP in some of their responses, NRS GROUP works every day to improve their services and satisfy the needs of his users and consumers. NRS GROUP always offers a quality service to generate and retain business and users' loyalty.

NRS GROUP worked and is working every day to offer its customers the best Service possible and to do so, NRS GROUP cooperates with partners to which NRS GROUP requires to be compliant as stated by NRS GROUP in its response dated October 6th, 2017.

"As you can see, from NRS we work every day to improve our services and satisfy the needs of our users. The company what it tries to offer is a quality service so that the customers stay much more time subscribed to our services [...]. In this moment we are working with very few Partners in this market for this main reason because we want to only work with those companies who can guarantee legit traffic and control on their traffic"

For the promotion of Applicateka, NRS GROUP cooperates with a lot of agencies in order to promote the Service as reflected from the contracting system of NRS GROUP explained above. Regarding the content locking issue, we can affirm that NRS GROUP has had problems with just two agencies (Affiliate 1 and Affiliate 2) that did not follow the instructions given and the agreement signed and the communications with requirements provided by NRS GROUP. The problems with the content locking are explained in this response.

It is very important to bear in mind that NRS GROUP employed different techniques and mechanism of control to prevent any breach of the English Law and the Code. Therefore, NRS GROUP has had a very high level of control over the actions performed by the agencies. Despite the control executed and restrictions given by NRS GROUP and the endeavours employed, it was materially and absolutely impossible to have 100% control over all the actions carried out by all the agencies, especially if the agencies do not comply with the agreement, the restrictions, the English law and the Code, which they are obliged to do.

The PSA pointed out two apparent scenarios of content locking related to the promotion of Applicateka in its Warning Notice dated April 23rd, 2019. Neither of those content locking scenarios were approved nor authorized nor known by NRS GROUP. For this reason, those apparent breaches should not be allocated to NRS GROUP, taking into account that NRS GROUP had implement the control systems explained above.

The first content locking mentioned in the document *"Details of apparent breaches of the Code"* was promoted by the agency Affiliate 1.

The content locking carried out by Affiliate 1 was, as stated by NRS GROUP in its response of May 18th 2017, not approved by NRS GROUP: *"it was a content locking that although was not approved by NRS GROUP, user was redirected to a landing page approved and where user was clearly informed of the service offered, as well as the costs associated to the service"* and, thus, could not be done and performed by the agency Affiliate 1 and was completely against any instruction received by NRS GROUP.

Moreover, NRS GROUP was never aware that this type of promotion was being executed because it is unimaginable that an agency of NRS GROUP could conduct such behaviour and promote a campaign that it was not only against the continuous instructions and obligations given by NRS GROUP, but also against the English law and the Code. NRS GROUP sent communications to Affiliate 1 explaining that the use of content locking was completely banned.

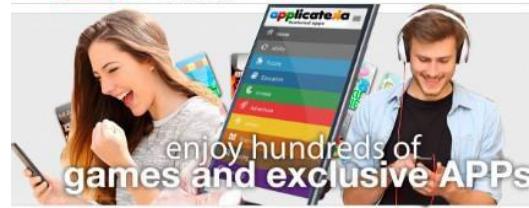
NRS GROUP, at the moment it realized that Affiliate 1 was using content locking, stopped all the collaborations and the different campaigns with Affiliate 1, blocking all the URLs involved on the incident: (i) <http://gta5hacktool.com> and (ii) <http://fifa17coins.com> and (iii) <http://nohumanverification.com>. NRS GROUP proceed to unsubscribe all the users affected and made the refunds through the MCOM pay-out service, as NRS GROUP stated on its response dated October 6th, 2017 and, thus, the users are not billed:

"Regarding promotion founded on Content Locking website on May 2017 we immediately blocked the URL involved on the incident and we also stop all activity with the Partner in the UK market. We didn't work with them since them. About the users affected with the promotion we unsubscribed all them and we make the refunds though the MCOM payout service"

Controlling Agencies, responsibility and reasonable endeavours

In addition to what it is mentioned above, NRS GROUP, giving due regard to transparency, has always presented users with vital information about the Service, (i) specifically regarding that it is a subscription service, (ii) informing about the price (before purchasing anything or subscribing), (iii) on how to unsubscribe properly from the Service and (iv) offering a 24/7 customer service via mail and telephone.

The information is shown before subscribing to the Service (as shown in the Fig. 5) and after subscribing (as shown in Fig. 6). The information presented to users is the following: *"Service for +18 users only. All minors under 18 are not allowed to subscribe or use the service. This is a subscription service costing £4.50 per week until you sent STOP to 64055. If you choose to enjoy the content form the service, you will enter into the subscription. By signing up for this service you agree that you are 18+ and have the permission of the account holder. You also acknowledge the you have read the Terms & Conditions. For help, please call 0203129 2986 or contact [info@nrs- group.com](mailto:info@nrs-group.com).*



Join or Subscribe to Applicatexa for £4.50 per week. You acknowledge that you have read the terms and condition.

SUBSCRIBE

Service for +18 users only. All minors under 18 are not allowed to subscribe or use the service

Service for +18 users only. All minors under 18 are not allowed to subscribe or use the service. This is a subscription service costing £4.50 per week until you send STOP to 64055. If you choose to enjoy the content from the service you will enter into the subscription. By signing up for this service you agree that you are 18+ and have the permission of the account holder. You also acknowledge the you have read the [Terms & Conditions](#). For help, please call 020 3129 2986 or contactinfo@nrs-group.com

Congratulations! Thanks for joining

You subscribed to Applicatexa with the phone number

Register to play

Service for +18 users only. All minors under 18 are not allowed to subscribe or use the service. This is a subscription service costing £4.50 per week until you send STOP to 64055. If you choose to enjoy the content from the service you will enter into the subscription. By signing up for this service you agree that you are 18+ and have the permission of the account holder. You also acknowledge the you have read the [Terms & Conditions](#). For help, please call 020 3129 2986 or contactinfo@nrs-group.com

Fig. 5: Screenshot of the subscription page with all the information for consumers (Annex 3 page 216) *Fig. 6: Screenshot of the subscription page with the information for consumers (Annex 3 page 180)*

NRS GROUP has always defended fairness and, as demonstrated in the several communications with PSA, has always prohibited and forbidden unfair and misleading content to its Agencies.

NRS GROUP is a Spanish company and hence its headquarters are in Spain. As the PSA already knows, NRS GROUP has engaged various companies to support them in controlling and ensuring the correct perform of the marketing. In order to do so, NRS GROUP hired the services of Empello Ltd, as a security company who provides anti-fraud monitoring, with the aim of having the maximum security and control of the content and to get alerts whenever there is a bad proactive, making sure that the agencies were neither advertising on any of the manners not authorized nor in the sites not authorized in order to avoid misleading and to guarantee that NRS GROUP have sufficient control and oversight on the promotion of the Service.

The above not only reflects the permanent good faith of NRS GROUP but its diligence when working in other countries by surrounding itself with partners and companies that guaranteed fulfilment of the agreement, the English law, the Code and Guidance. Indeed, NRS GROUP stated so in its response dated May 18th, 2017:

"Given our interest in having high standard of compliance in the countries we operate, and also given the fact that being out of the UK is almost impossible to monitor campaigns in the same detail as per the companies with local presence in the country, we hire Empello services to monitor and give us alerts when they detected a bad proactive."

Providers, as stated in the "Promoting Premium Rate Services Guide", should use all reasonable endeavours when subcontracting to affiliates and retain responsibility from the campaigns. In its activity, NRS GROUP has been aware of its responsibility to ensure that the promotions were compliant with the English law and the Code. Therefore, NRS GROUP as previously mentioned, has always put in place appropriate controls to ensure the agencies were compliant, giving recommendations, establishing restrictions and performing an internal protocol of control. In order to strengthen its control over the agencies, NRS GROUP engaged the services of a third-party company to deploy all its reasonable endeavours to comply with the English law and the Code.

Therefore, all what we have explained above demonstrate that NRS GROUP has complied with all the responsibility and control exigences proactively and diligently, always with its priorities clear, this is to say: protect the consumers, be surrounded with compliant partners and offer a transparent and fair service, which, NRS GROUP always has done. NRS GROUP had imperatively obliged the agencies to follow the obligations and restrictions given, if the agencies by their sole determination, decide not to follow said obligations, seems disproportionate to fully or partly blame NRS GROUP.

Monitoring the content locking of the promotion carried out by Affiliate 2

The second content locking scenario pointed out by PSA was related to a promotion carried out by the agency Affiliate 2. The PSA wants to allocate the apparent breach of the Code to some actions that, as said before, were neither carried out nor authorized nor approved and nor known by NRS GROUP.

The PSA conducted a monitoring of a promotion of Applicateka that apparently took place in August 2018 due to a complaint of the parents of an underage user that subscribed to Applicateka once he saw a YouTube video that redirected this user to a website www.clashroygems.cf. The aforementioned website was related to the game Clash Royale which is a free videogame with in- game purchases in form of gems and golden coins.

The game combines elements of collectible card games, tower defence and multiplayer online battle arena. The YouTube video (object of the monitoring) indirectly, redirects users to the website www.clashroygems.cf which apparently suggested that users could obtain gems and golds for free.

The agency responsible for the promotion carried out through the website shown in the YouTube video was, as stated above, Affiliate 2. Said agency did neither have the authorization nor the approval to do said promotion and therefore, it is the sole responsible.

Moreover, as declared by NRS GROUP in one of the responses, it was not aware that this type of promotion was being executed because it is unimaginable that an agency of NRS GROUP

could conduct such behaviour and promote such campaign that its, by all means, not only against the agency agreement signed with NRS GROUP and the continuous instructions and obligations, but also against the English law and the Code. As stated by NRS GROUP in its response dated October 6th, 2017: *"we want to make completely clear that NRS GROUP was not aware of this type of promotion, and it was solely performed by the advertising agency without our control or authorization. We always inform our Partners about all the compliancy rules"*

But also, at the moment NRS GROUP was aware about the content locking by Affiliate 2, NRS GROUP decided to stop all the campaigns carried out by Affiliate 2 in the UK.

The abovementioned promotion, carried out through the YouTube video, was solely performed by the agency Affiliate 2 without the permission and control of NRS GROUP. Either EMPELLO LTD was aware that this promotion was being held by the agency Affiliate 2 and hence, could not advise NRS GROUP on the misbehaviour of the promotion.

NRS GROUP wants to make clear that it is fully against any conduct that may harm the consumers and it is a priority to NRS GROUP to be compliant with the English law and the Code.

Immediately after acknowledging said promotion, NRS GROUP cut the link to the website www.clashroygems.cf of the agency Affiliate 2 involved and informed him that that kind of incentive traffic is not allowed and therefore, the Affiliate 2 must, instantly, deliver the content promised to the user in the moment of the subscription. Affiliate 2 assured that he sent a PDF file where tips and tricks were offered to the users. We consider that the information provided, exclusively by Affiliate 2, in said PDF was of help to the users as it helped them to understand better the way Clash Royal game works and can give users ideas to start making great strategies in order to get more rewards and win battles against their opponents.

However, and even if the agency did the promotion without the knowledge and consent of NRS GROUP and sent a PDF file with tips and tricks, NRS GROUP proceeded to fairly unsubscribe all users from the Service and made immediately the refund through the MCOM Service."

The Level 2 provider also made oral representations to the Tribunal. The Level 2 provider reiterated the written representations made by its legal representatives.

In response to questioning by the Tribunal, the Level 2 provider stated that the service had commenced in 2015 and had also been registered with the PSA since 2015. It confirmed that it had approximately 50 employees and operated in multiple jurisdictions.

The Level 2 provider stated that its goal was to offer a diversity of content with added value to all users, and that the Level 1 provider had been recommended to it as the best aggregator to monetise game content in the UK. The Level 2 provider stated that it had put in place solid agency agreements with its marketing partners, including a prohibition on content locking, and it had made clear that traffic restrictions had to be complied with. The Level 2 provider disputed that it had used content locking at any time as a form of promotion and confirmed that it had never asked any marketing agency to deploy such tactics and that there was no

evidence before the Tribunal of this. The Level 2 provider stated that, when it had become aware of the content locking, it had ceased its relationship with the marketing agency concerned. The Level 2 provider stated that its responsibility as a company was to protect consumers and to offer fair and transparent services and in its view this was always the case.

The Level 2 provider proceeded to play a short video clip to the Tribunal showing a user journey for the service, including the terms and conditions visible to the user together with information on how a user could cancel the service.

The Level 2 provider stated that it had issued refunds to consumers in the sum of £14,245, but that this had not been taken into consideration by the Executive. The Level 2 provider stated that it did not understand why the Executive had recommended the maximum fine available for the breach rather than, for example, a warning not to repeat the conduct, when what had occurred was outside of its control and it had already shown this.

The Level 2 provider stated that its proposal was that no sanction should be imposed in light of the following facts: that no responsibility for the breach could be attributed to it, that it had solid contracts in place with all marketing partners, that it had fully co-operated with the Executive's enquiries throughout, that it had issued full refunds to users, suspended the service and unsubscribed all users. The Level 2 provider asked that, in the alternative, if the breach was made out, that all these facts be taken into consideration.

3. The Tribunal considered the Code and all the evidence before it. The Tribunal considered that the Level 2 provider had effectively admitted that the breach had occurred, noting that the Level 2 provider's representations did not amount to a defence but instead focussed on where responsibility for the breach lay. On this point, the Tribunal was satisfied that the Level 2 provider was responsible for the actions of its marketing partners and that the PSA's Guidance on 'Promoting Premium Rate Services' made it clear that providers were ultimately responsible for the actions of their affiliates and that all providers should exercise caution in controlling the risks of affiliate advertising.

The Tribunal was satisfied, for the reasons advanced by the Executive, that consumers had in fact been misled into entering the service on the promise of virtual currency and that the promise of virtual currency had not been delivered. The Tribunal considered that the PDF guide provided to consumers was not an adequate substitute for what had been promised in the form of virtual currency and was of the view that the PDF was of no value to consumers.

The Tribunal noted the Level 2 provider's representations that it had not instructed the marketing agency to engage in prohibited activities and the Tribunal accepted that the Level 2 provider did have contracts in place prohibiting such practices. Nonetheless, the Tribunal considered that it remained the responsibility of the Level 2 provider to ensure that its marketing agency delivered what had been promised to consumers. The Tribunal's view was that the evidence demonstrated that the Level 2 provider had not gone to all lengths possible to resolve this issue, as there was no evidence that the Level 2 provider had done any more than have contracts in place,

despite having been issued previous warnings or 'yellow cards' by the mobile networks. The Tribunal considered that this should have resulted in the Level 2 provider being cognisant of content locking as a potential issue and should have alerted the Level 2 provider to the need to monitor and control the activities of its affiliates more closely, which it did not appear to have done.

The Tribunal was satisfied on the balance of probabilities that consumers had been misled into entering the service and accordingly upheld a breach of rule 2.3.2 of the Code.

Decision: UPHELD

Alleged breach 2

Rule 2.3.3 of the Code states:

"Consumers must not be charged for PRS without their consent. Level 2 providers must be able to provide evidence which establishes that consent."

1. The Executive stated that it believed that the Level 2 provider had breached rule 2.3.3 of the Code because consumers were signed up to the Service without their consent.

The Executive relied on the content of the PSA Guidance on 'Consent to Charge'.

The Guidance states:

"1.1 Premium rate services allow a charge to be generated to a consumer's phone bill, whether pre-paid or post-paid as part of a contract with an originating network, directly and remotely. A major concern then is that they can be charged without having requested or consented to any purchase."

1.2 It is important to understand the need for transparency when establishing any consent to charge a consumer via PRS payment. The key service information necessary to comply with rule 2.2.4 of the Phone-paid Services Authority's Code of Practice must be presented clearly and with suitable proximity and prominence. This is to ensure any action on the consumers part reflects a genuine intention to consent to the charges triggered by the action."

On 2 October 2018, the Level 1 provider had informed the Executive that it was in the process of refunding Net Real Solution consumers that had been the victims of "malware" (short for "malicious software").

The Executive asked the Level 1 provider to supply further details regarding how the malware issue had been identified. The Level 1 provider responded as follows:

“Malware was identified on a separate service and a review was then carried out of all services to identify whether any others had been affected. This was done by way of a report being generated that identified whether all three stages of the subscription process had been properly followed. In this report it was identified that NRS Applikateka was a service that had been affected.”

Based on the user flow that was supplied by the Level 2 provider, a consumer would normally be required to actively perform a number of actions to initiate a subscription. These included:

1. User clicks on the banner
2. User access to the promotion
3. User click the Subscribe button and is redirected to the carrier billing page and accepts the terms and conditions
4. User is subscribed

The Executive sought to gain a better understanding of the malware issue and the Level 1 provider provided the following information:

“The malware affected the customer’s website whereby it allowed the merchant to raise a request for a new service, at this point before the page was loaded, the malware intercepted the url to Consent page and change it effectively to create a successful subscription.

By doing this the malware enabled the request to skip the first two pages of the payment flow (call-to-action and confirm-action) and call the create action (this is where the subscription is created) directly.”

The Executive submitted that it possessed limited information regarding precisely how the malware functioned. However, the Executive noted that, according to the Level 1 provider, the malware had the effect of bypassing steps two and three of the user flow as outlined above, namely “user access to the promotion” and “user clicks to subscribe”. The Executive stated that these were the steps that effectively obtained a consumer’s consent to be charged.

The Executive had asked the Level 1 provider to confirm how many consumers had been affected by the malware issue and the Level 1 provider had supplied a report detailing that 33,450 consumers had been subscribed to the Service without the required consent between 1 May and 16 July 2018. The Level 1 provider had notified the Level 2 provider on 31 July 2018 that it had suspended the Service because of the malware issue.

The Executive asked the Level 1 provider if it had identified the source of the malware. The Level 1 provider advised that the source of the malware was the affiliate partner Affiliate 3.

The Executive stated that Code Guidance on 'Digital marketing and promotions' confirmed that the responsibility to control affiliate marketing lay with the Level 2 provider:

"1.5 This Guidance also clarifies that it is the responsibility of providers to control affiliate marketing carried out on their behalf and sets out some recommendations as to how to do so safely. For further assistance on controlling risk when using affiliate marketers please read part 10 of the 'Promoting premium rate services' Guidance."

In addition, Part 10 of 'Promoting Premium Rate Services' Guidance – Controlling risk stated:

"10.2...the Phone-paid Services Authority recognises that the Level 2 provider, while retaining responsibility for the promotion under the Phone-paid Services Authority's Code of Practice, may not have immediate, day-to-day control of each individual action that an affiliate takes. However, the use of affiliates to market PRS products on a provider's behalf does carry a greater risk than marketing which is under the direct, day-to-day control of the provider. For further detail around affiliate marketing, please see the General Guidance Notes on 'Digital Marketing' and 'Due Diligence Risk Assessment and Control'."

The Executive had considered the controls the Level 2 provider had put in place regarding its use of affiliates. In response to a direction for information, the Level 2 provider had sent the Executive a copy of the Advertisement Agreement between the Level 2 provider and Affiliate 3. The agreement was signed on 31 December 2015.

The Level 2 provider's legal representative stated that the agreement included prohibitions for the affiliate marketer and referred to the following extract of the agreement:

"2) The following forms of advertising are completely banned for NRS-Group campaigns in all the markets. The advertising network agrees and understands that none of the below advertising methods are allowed. Techniques no listed in the approved list should not be used until they are explicitly approved via email by NRS - GROUP:

[...]

Anything which is misleading, including creating a false sense of urgency (e.g. countdown clocks, statements of limited availability) or making promises that cannot be delivered;

Unsolicited email, SMS or other messaging;

Collecting mobile

number or other personal information from the consumer without their consent; Any viruses, malware, spyware or other malicious or harmful code;"

The Level 2 provider's legal representative further stated to the Executive that:

"Affiliate 3 signed the Advertising Agreement and the General Terms and Conditions so it was fully aware of its obligations and prohibitions regarding any malware or malpractice and was obliged to guarantee its compliance with national advertising legislations, especially in the United Kingdom."

Further to the above, the Level 2 provider's representative supplied copies of correspondence between the Level 2 provider and Affiliate 3. The Level 2 provider's representative stated that, in the emails dated 31 May 2018 and 14 June 2018, the Level 2 provider had reminded Affiliate 3 of the *"restrictions applicable aside from limits agreed between the parties in the Advertisement Agreement"*.

The Level 2 provider's legal representative further stated that the following restrictions were outlined for UK promotions within the emails:

" Restrictions:

- No incent traffic.*
- No websites related with kids.*
- No content locking*
- Don't use banners not reviewed by the advertiser*
- No social traffic*
- No redirects."*

The Executive noted that the Level 2 provider made no reference to the restrictions outlined in the Advertising Agreement and the Executive relied on section 2 of the Digital marketing and Promotions Guidance which states:

2.3 Providers therefore must put in place appropriate controls to ensure their affiliate marketing adheres to the Code as part of their ongoing compliance processes. The absence of any such mechanisms may be viewed by a Phone-paid Services Authority Tribunal as a failure of the provider to assess the potential risks posed by a party with which they contract and maintain steps to control these risks.

The Executive submitted that its expectation was that the Level 2 provider, as part of its on-going controls over its promotions, would remind its advertising partners of the full restrictions that applied and ensure, through regular checks and monitoring, that the restrictions were being complied with. The Executive considered that this would have been especially prudent given the problems the Level 2 provider had experienced with affiliate marketing in the area of content locking. In addition to this, the Executive stated that the Level 2 provider should have been alive to the need to increase its monitoring of its promotions given the upsurge in its subscriptions, which amounted to 33,450 new consumers subscribing between 1 May and 16 July 2018

and also the increase in complaints being referred to the Level 2 provider by the Executive, which amounted to 452 complaints between May and June 2018.

The Executive asserted that a simple prohibitory clause in an affiliate agreement was not sufficient, in the absence of other service monitoring and controls, to detect and mitigate the risks to service users. As such, it was not sufficient for the Level 2 provider to rely on a document that had been signed in 2015 to fulfil its ongoing responsibility to ensure that its advertising partners were complying with the Code.

The Executive relied upon section 3 of the General Guidance Note – ‘Due diligence; risk assessment, and control on clients’, which outlined questions for the Level 2 provider to consider when dealing with affiliates, including around post-contract monitoring, risk assessment and control. The Executive stated that matters for a Level 2 provider to consider were as follows:

Post-contract Monitoring, Risk Assessment and Control
<ul style="list-style-type: none">• Is my monitoring systematic and does it give me a good understanding of how my customers are being drawn to my service?• Do I have the appropriate controls in place to ensure that any unusual activity is identified quickly?• Am I analysing all aspects of this relationship, including customer complaints?• Given the risks associated with affiliate marketing, can I demonstrate that my monitoring is sufficient, thus adequately mitigating those risks?

The Executive stated that the Level 2 provider’s representative had supplied copies of Skype conversations between Affiliate 3 and the Level 2 provider, relying upon a Skype conversation of 12 July 2018 as evidence of when the Level 2 provider first had suspicions regarding the malware issue. However, having reviewed the conversation, the Executive considered that this was not borne out by the Skype conversations, which related to issues other than malware. The Executive noted that it appeared that the Level 2 provider had informed Affiliate 3 that it had paused the affiliate marketer’s promotion on the basis that the affiliate marketer had used “*generic banners*” in line with the restriction “*Don't use banners not reviewed by the advertiser*”. While the Executive noted that the Level 2 had paused its promotion of the Service, it was not apparent, based on the evidence supplied, that this was as a result of an awareness of the malware issue.

The Executive further noted from the Skype conversations supplied that the Level 2 provider had reminded Affiliate 3 that promoting on *"kids YouTube is strictly forbidden"* as it was a *"restricted practice"* but that the Level 2 provider had made no mention of malware being a restricted practice.

The Executive stated that it therefore did not agree that the evidence submitted by the Level 2 provider's legal representative demonstrated that the Level 2 provider had been monitoring the Service, including the issue of malware, sufficiently.

The Executive submitted that a total of 33,450 consumers were subscribed to the Service without their consent as a result of inadequate control by the Level 2 provider over the affiliate marketing of the service.

Accordingly, the Executive submitted that a breach of rule 2.3.3 of the Code had occurred.

2. The Level 2 provider denied the breach and its legal representative submitted the following written representations on its behalf:

The Executive asserts that NRS GROUP has breach rule 2.3.3 of the Code on the basis that consumers of Appicateka have been subscribed to the Service without, apparently, their prior consent.

Vulnerability of the payment platform the Level 1 provider

During the investigation process on the Appicateka Service carried out by the PSA, the latter exchanged some communications and information with the Level 1 provider about what happened between May and July 2017.

NRS GROUP with the purpose of promoting the Service in United Kingdom correctly, hired the services of the Level 1 provider which is the company that offers the payment system and provides a messaging aggregation and management services connexion (*sic*) needed to operate in the United Kingdom.

In the communications mentioned in the first paragraph, the Level 1 provider assumed the responsibility and acknowledged the vulnerability of the payment platform, which due to its vulnerability allowed the creation of subscriptions without the need to consent said subscription. The non-consented subscription was exploited through the use of malicious programs. As stated (to the Executive) *"We know that the Level 1 provider's vulnerability (allowing subscriptions to be created without confirm action) was exploited through the use of malware, but it was also possible to exploit by other means"*.

In the same period, NRS GROUP detected another failure of the payment platform of the Level 1 provider that re-subscribed users that had been already and previously

unsubscribed. As stated (to the Executive): *"This is because those subscriptions were re-subscribed and the created at time was modified for re-billing purposes. The first_Billing_Created_At column will contain the real subscription date"*. Afterwards, NRS GROUP informed the Level 1 provider about it and, afterwards, decided voluntarily to terminate the collection process of its entire data base until the malware problem was solved and pausing all the campaigns which were affected by the malware, as shown in a skype conversation with Affiliate 3, attached in NRS GROUPS's response dated 20th December, 2018.

The actions described above and carried out by NRS GROUP not only exhibit the good faith, proactivity and diligence undertaken in the good work of NRS GROUP but also determines that the priority of NRS GROUP was not to harm the users and to solve as soon as possible the eventual damages by refunding and unsubscribing the users from the Service.

Therefore, the sole responsible parties for said malware were (i) the Level 1 provider aggregator and (ii) the United Kingdom operators who should have ensured that their payment platforms were secure and that they had the necessary mechanisms to detect that users passing through their payment platform effectively completed all the steps of the payment process until a successful transaction.

We can affirm without any doubt that the malware was not a problem of NRS GROUP. Since the very first moment in which NRS GROUP became aware of the malware, NRS GROUP decided to cut the traffic and initiate an investigation by its own means. All the users that NRS GROUP suspected that could have been affected by the malware were immediately unsubscribed and funds were refunded.

If the malware was neither noticed by the Level 1 provider nor the aggregator nor Empello, it was impossible for NRS GROUP to notice or either foresee its occurrence as it was beyond its control. Thus, it is incredible that a punitive financial sanction might be applicable and upheld against NRS GROUP which employed more than the reasonable endeavours:

(i) to prevent that users are harmed, (ii) to control risks and (iii) to ensure the promotions were compliant with the Code and the English law. The actions taken by NRS GROUP were always diligent and compliant with the Code, solving the damages immediately.

NRS GROUP has always been available to cooperate in the investigation conducted by PSA and facilitated all kind of information and documentation that may help shed light into the malware issue that was happening and that could at some point incur future problems.

NRS GROUP is not responsible for the payment method, NRS GROUP hired the payment process to the Level 1 provider, which was in charge of providing a secure and transparent payment system. The problem with the non-consented subscription and, therefore, the billing, was out of the system of NRS GROUP and completely out

of their reach. NRS GROUP could only warn the aggregator to solve the problem as soon as possible and reduce the damage to users. Neither the Agency, nor the Level 1 provider, could have explained and proved how the malware acted.

Appropriate control over the Agency

NRS GROUP has always been clear with its partners and has always put in place appropriate controls to ensure that its agencies were compliant and that did not proceed with unauthorized practices. In various communications that NRS GROUP maintained with the agency responsible of the malware, Affiliate 3, it has always pointed out what actions were totally forbidden and to be compliant not only with the agreement but also with the English law and the Code.

- 2) *The following forms of advertising are completely banned for NRS-Group campaigns in all the markets. The advertising network agrees and understands that none of the below advertising methods are allowed. Techniques not listed in the approved list should not be used until they are explicitly approved via email by NRS-GROUP:*
- [...]*
- ***Anything which is misleading**, including creating a false sense of urgency (e.g. countdown clocks, statements of limited availability) or making promises that cannot be delivered;*
 - *Unsolicited email, SMS or other messaging;*

Fig. 8: Extract from Affiliate 3 agreement

The Agency, Affiliate 3, agreed to conduct due diligence on all traffic sources, control and assess the affiliate fraud, understand the compliance and advertising regulation of each market and establish a notification and reporting facility. Likewise, Affiliate 3 acknowledged that any kind of virus or malware was a non-permitted technique and it is completely banned.

The list of prohibitions and restrictions that NRS GROUP apply and impose to an Agency is unlimited and non – exhaustive. This means that the only requirement that always applies to an agency when promoting the Service is that the techniques and means employed must be compliant with the English law and, hence, the Code. The Agencies, particularly Affiliate 3, are fully aware of its obligations and prohibitions regarding any malware or malpractice and their obligation to guarantee compliance with English advertising law, especially in the United Kingdom.

As stated in NRS GROUP's response dated 20th December, 2018, the Level 1 provider has been hired to provide a payment system and the connexion (*sic*) needed to operate in United Kingdom, furnishing security and trust on all other partners and a main filter avoid illicit content or any malware. As stated:

"In order to provide a satisfying service though Applicateka [...] NRS GROUP hired the services of the Level 1 provider which is a company that offers the payment system and the connexion needed to operate in the United Kingdom"

This is to say that, NRS GROUP, to operate in the United Kingdom, need to be surrounded with responsible, diligent and compliant companies to trust that they will, in every way, control and develop their functions accordingly to the agreement, the English law and the Code.

Either way, the subscription process of NRS GROUP meets all the legal requirements. When any users arrive to the landing page of the Service, he/she is informed adequately of the price, the subscription service offering to them, the existence of a customer service 24/7 and the process to unsubscribe correctly from the Service. NRS GROUP's goal is to satisfy all the consumers by offering quality content so that the services meet the expectations of users seeking their own satisfaction and to guarantee that they stay loyal as long as possible enjoying the Applicateka content.

According to all the above, we can affirm that NRS GROUP, in the interest of protecting the consumers and being compliant with the Code, has acted diligently and controlled the agencies and partners based on the means available and employing more than the reasonable endeavours."

The Level 2 provider also made oral representations to the Tribunal. The Level 2 provider reiterated the written representations made by its legal representatives.

In response to questioning by the Tribunal the Level 2 provider stated that the Level 1 provider had been recommended to it as a reputable aggregator in the UK market. The Level 2 provider stated that it only became aware that malware had affected the Level 1 provider's platform when it saw the email the Level 1 provider had sent to the Executive in the hearing bundle, explaining that malware had affected its system. The Level 2 provider stated that it had come as a great surprise that this vulnerability existed and that the responsibility for this issue rested solely with the Level 1 provider, whose platform it had trusted. The Level 2 provider stated that, when it became aware of the issue, it had acted in good faith by suspending all promotions of the service and it had conducted its own investigation, before receiving the internal communication between the Level 1 provider and the Executive. Its intention had never been to harm users, but rather to resolve the issue by refunding them and unsubscribing them from the service and all funds had been refunded. The Level 2 provider stated that these facts had not been adequately considered in the fine being recommended by the Executive. The Level 2 provider did not agree that a fine should be imposed because, in circumstances where the malware had gone unnoticed by the Level 1 provider and the Mobile Networks, it was impossible for it to control the issue.

The Level 2 provider stated that in total it had issued £104,000 in refunds and that, although it might appear that it had made a lot of money from the service, this was not the case as after investments in marketing it had, in fact, made a loss.

The Level 2 provider stated that its proposal was that no sanction should be imposed in light of the following facts: that no responsibility for the breach could be attributed

to it and that the responsibility lay solely with the Level 1 provider, that it had shown commitment to ensure good processes by having contracts in place with its marketing partners and by contracting with the monitoring house, Empello, that it had fully co-operated with the Executive's enquiries throughout, that it had issued full refunds to users, suspended the service and conducted its own investigation and unsubscribed all users. The Level 2 provider asked that, in the alternative, if the breach was made out, that all these facts be taken into consideration.

3. The Tribunal considered the Code and all the evidence before it. The Tribunal noted that the Level 2 provider had accepted that consumers had been charged without consent but claimed that it was not responsible.

Although the Tribunal noted the Level 2 provider's representations that the Level 1 provider was the party responsible for the malware issue, the Tribunal considered that the ultimate responsibility for ensuring that consumers were not charged without consent rested with the Level 2 provider, who had contracted with the marketing affiliates. The Tribunal was satisfied that the Level 2 provider had not adequately monitored and controlled the risks of the affiliate marketing of the service and was of the view that it was not sufficient to simply have a contractual prohibition in place, in the absence of other regular controls and monitoring.

The Tribunal considered the matter to be very serious in terms of the scale of the harm, noting that a very large number of consumers had been affected. The Tribunal's view was that, given that 33,000 consumers had been signed up to the service without their consent and that this had led to a corresponding upsurge in subscriptions and complaints, this should have alerted the Level 2 provider to this matter. The Tribunal considered that the issue could and should have been detected and acted upon more quickly by the Level 2 provider. The Tribunal expressed concern that, even after the Level 2 provider had been made aware of the malware issue, the evidence showed that it had continued to tell consumers that they had agreed to sign up to the service.

The Tribunal was satisfied on the balance of probabilities that consumers had been charged for the service without their consent and accordingly upheld a breach of rule 2.3.3 of the Code.

Decision: UPHELD

Sanctions

Assessment of breach severity

1. The Executive assessed the severity of the breaches as follows:

Rule 2.3.2 – Very Serious

Rule 2.3.2 - Very Serious

2. The Tribunal assessed the severity of the breaches as follows:

Rule 2.3.2 – Very Serious

The Tribunal considered that the breach had the potential to severely damage consumer confidence in phone-paid services and that the breach had been committed recklessly. In reaching this decision the Tribunal considered that the Level 2 provider was aware that content locking was a potential risk in the promotion of the service as a result of having received notifications from the mobile networks previously that content locking had affected the service, yet it had not taken adequate steps to monitor and control that risk.

Rule 2.3.3 - Very Serious

The Tribunal considered that the breach would have had a clear and detrimental impact on consumers of the service and that the service had the potential to severely damage confidence in the phone-paid services. Consumers had also incurred a wholly unnecessary cost. The Tribunal considered that the breach had been committed negligently in that the Level 2 provider had failed to adequately control the risks of the marketing of the service.

The Tribunal's initial assessment of the breaches of the Code was that they were, overall **Very Serious**.

Initial assessment of sanctions

The Executive's initial assessment, before any potential uplift or downgrade in light of aggravating or mitigating features, was that the following sanctions were appropriate based on a preliminary assessment of the breaches as "very serious":

- a requirement to remedy the breach by ensuring that malware affected consumers should not be re-subscribed to the service and/or other services operated by the provider
- a formal reprimand
- a requirement that the Level 2 provider must submit all promotional material for all services which are being (or will be) promoted via affiliate marketing to PSA for compliance advice for a period of 2 years
- that access to the Service be barred for a period of 6 months pending PSA supplying compliance advice on any existing or proposed future promotions that are marketed via affiliates
- a requirement that the Level 2 provider refund all consumers who claim a refund
- a fine of £500,000 comprised as follows:

Rule 2.3.3 - £250,000

Rule 2.3.2 - £250,000.

The Level 2 provider accepted the proposed compliance advice sanction but did not accept the proposed bar on access to the service on the basis that it did not consider that it had breached the Code or engaged in any illegal activity. With regard to the proposed refunds sanction, the Level 2 provider stated that refunds had already been issued. The Level 2 provider did not agree with the initial fine sanction for the reasons stated in its representations in respect of the breaches.

The Tribunal agreed with the Executive's initial assessment of sanctions, save that:

- the Tribunal did not agree that the remedy the breach and compliance advice sanctions should apply to any other service other than the service which was the subject of the proceedings
- the Tribunal considered that a bar on access to the service should be for 2 months rather than 6 months.

Proportionality assessment

Assessment of mitigating and aggravating factors

Mitigation

The Executive submitted that there were the following mitigating factors:

- the Level 2 provider had ceased the content locking journeys when notified by the PSA
- the Level 2 provider had severed ties with the affiliate marketers responsible for the content locking.

The Level 2 provider stated that the following were mitigating factors:

- it had used more than reasonable endeavours to control its marketing partners
- it had taken steps in advance to identify and mitigate against external factors that might result in breaches, as outlined in its response to the breaches
- refunds had been proactively made to consumers and all users had been unsubscribed from the service

- it had cooperated fully with the PSA investigation
- it had terminated its agreements with the marketers responsible for the non-compliant promotions and cancelled all campaigns, as outlined in its response to the breaches
- it had taken all reasonable steps, techniques and mechanisms to control and mitigate any breach of the Code.

The Tribunal found the following mitigating factors:

- the Level 2 provider had ceased all content locking journeys when notified by the PSA
- the Level 2 provider had proactively issued refunds to all consumers affected by the content locking. The Tribunal did not accept however that the refunds issued to consumers affected by the malware were proactive as this were implemented by the Level 1 provider
- the Level 2 provider had taken steps to minimise the risk of breaches recurring by severing ties with the affiliate marketers responsible
- the Level 2 provider had secured the services of a monitoring house, which was evidence of some additional measure being taken to control risk.

The Tribunal did not agree with the Level 2 provider that it had gone beyond the level of co-operation with the Executive that is usually expected. Although it had cooperated adequately, this did not go beyond what was required under the Code. The Tribunal also did not agree that the provider took steps to identify and mitigate against the risk of external factors that might result in a breach of the Code, as there was no evidence of this other than contracts, which the Tribunal considered to be insufficient in the absence of other robust monitoring and control procedures.

Aggravation

The Executive submitted that the following were aggravating factors:

- the Level 2 provider has failed to follow Guidance on the promotion of phone-paid services and the control of affiliate marketers
- the Level 2 provider had been warned as early as 2016 about the use of content locking, but despite this the use of content locking continued to occur.

The Level 2 provider stated that there were no aggravating factors. It had not failed to follow Guidance for the reasons explained in its response and it was materially impossible to foresee what affiliate marketers would do. It had banned content locking with all marketers but despite all the restrictions, some marketers continued with the content locking, which caused them to immediately terminate its relationship with those marketers.

The Tribunal found that it was an aggravating factor that the Level 2 provider had failed to follow Guidance or exercise proper caution when engaging with affiliate marketers.

The Tribunal did not agree that it was an aggravating factor that the Level 2 provider had previously been warned about content locking as early as 2016. While the Tribunal noted that the mobile networks had made the Level 2 provider aware of previous incidences of content locking, there was inadequate evidential material in the bundle regarding any other warnings and it would not be proper to rely upon material that was not contained in the Warning Notice.

Revenue

The Executive stated that the estimated gross Level 2 provider revenue flowing from the breach of rule 2.3.2 was £24,640.20, based upon a calculation of the average consumer spend for a total of 1,053 affected users.

The Executive stated that the estimated gross Level 2 provider revenue flowing from the breach of rule 2.3.3 was £225,207.00, although the Executive noted that the Level 1 provider had retained this revenue in order to refund affected consumers.

In response to questioning by the Tribunal, the Executive clarified how it had arrived at the relevant revenue figure. The Executive stated that the figures represented the gross Level 2 provider revenue *generated* by the service as a result of the breaches of rules 2.3.2 and 2.3.3, and that the relevant time period when considering the breach of rule 2.3.2 was from January 2017 onwards. These figures did not take into account the revenue *received* by the Level 2 provider. However, the Executive did ask that the Tribunal take into account the revenue actually received by the Level 2 provider when considering the actual financial benefit to the provider and the appropriateness and proportionality of any final sanctions imposed.

The Level 2 provider stated that the revenue amounts calculated by the Executive did not take into account the refunds issued to consumers, which amounted to £14,245.40 in respect of the breach of rule 2.3.2, or the refunds issued in respect of the breach of rule 2.3.3, which had in total resulted it in sustaining a loss of £76,136.00. The Level 2 provider also stated that the Executive had not properly considered that the net revenue received by it in respect of the service was approximately 50% of the total revenue after costs.

The Tribunal's agreed with the Executive that the relevant revenue figure for sanctioning purposes was the total Level 2 provider revenue generated as a result of the two breaches, not the amount of profit, albeit the amount of revenue received by the Level 2 provider was a relevant proportionality consideration at final sanctions setting stage. The Tribunal also considered that it was entitled to consider the revenue generated from January 2017 onwards, after derogation was obtained from the Level 2 provider's home member state, and when the breach of rule 2.3.2 was occurring.

The Tribunal agreed with the relevant revenue figures supplied by the Executive, noting that although the figure was the gross Level 2 provider revenue generated, the financial benefit

to the Level 2 provider was in the region of £10,000 when taking into account the refunds issued to consumers and the monies withheld by the Level 1 provider and the Executive.

Financial benefit/ Need for deterrence

The Executive stated that as a result of the Level 1 provider suspending the service and voluntarily withholding the revenue derived as a result of the breach of rule 2.3.3 (consent to charge) the Level 2 provider had not actually received the financial benefit from these subscriptions and had overall received, taking into account the refunds made in respect of both breaches, approximately £10,000. Notwithstanding this, given the seriousness of the breaches, the Executive considered there to be a need to impose a financial sanction that marked the gravity of the breaches. The Executive stated that there was a need to impose sanctions that would be sufficient to prevent a reoccurrence of consumer harm of this nature in respect of the service and to deter the Level 2 provider and the wider industry from the future commission of such breaches.

The Level 2 provider stated that there was no need to remove the financial benefit as it had not benefitted from the revenue generated and that it had issued refunds to consumers affected by the content locking through a third-party company. The Level 2 provider stated that it no longer had any live campaigns and had terminated its relationships with those affiliates responsible for the breaches. The Level 2 provider stated that it was not appropriate or justified to impose the Executive's recommended sanctions.

The Tribunal agreed with the Executive that it was necessary to mark the very serious nature of the breaches, given the scale of the harm and the very large numbers of consumers affected. The Tribunal also considered it necessary to impose sanctions which were sufficient to prevent a reoccurrence of such breaches by the Level 2 provider, or by the wider industry. The Tribunal acknowledged that the Level 2 provider had only received approximately £10,000 in revenue, but nonetheless noted that a significant amount of revenue had been generated as a result of the breaches and the Level 2 provider's conduct, which had resulted in widespread consumer harm.

Sanctions adjustment

As the Level 2 provider had in fact received no revenue flowing from the breach of rule 2.3.3 (consent to charge), the Executive recommended that the initial fine sanction for the breach of 2.3.3 be adjusted downwards to reflect this from £250,000 to £25,000, in order to achieve a proportionate outcome.

The Tribunal agreed with the Executive that the initial fine amount for the breach of rule 2.3.3 should be adjusted downwards to £25,000 for the reasons advanced by the Executive.

The Tribunal also considered that, in light of all of the representations made by the Level 2 provider and upon consideration of the refunds issued by the Level 2 provider to those consumers affected by the breach of rule 2.3.2 (misleading), that it was also appropriate to adjust the initial fine sanction in respect of this breach downwards from £250,000 to £175,000.

Final overall assessment

Sanctions imposed

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

- a requirement to remedy the breach by ensuring that malware affected consumers should not be re-subscribed to the service
- a formal reprimand
- a requirement that the Level 2 provider must submit all promotional material for the Appicateka service, which is being (or will be) promoted via affiliate marketing to PSA for compliance advice for a period of 2 years
- that access to the Service be barred for a period of 2 months pending PSA supplying compliance advice on any existing or proposed future promotions that are marketed via affiliates
- a requirement that the Level 2 provider refund all consumers who claim a refund
- a fine of **£200,000** comprised as follows:

Rule 2.3.2 - £175,000

Rule 2.3.2 - £25,000.

Administrative charge recommendation: 100%

ANNEX A

Application for interim measures pursuant to Code of Practice paragraph 4.6

Case reference: 134234

Level 2 provider: Net Real Solutions SLR

Type of service: Multi-media subscription service

Service name: Appicateka

Network operator: all mobile network operators

Cost: 4.50 per week

PRNs: N/A

1. This is an application by the Phone-paid Services Authority's (the "**PSA**") Executive seeking a direction in accordance with paragraphs 4.5.1(b) and 4.6.2 and 4.6.5(c) of the PSA Code of Practice (14th edition) (the "**Code**") that up to £115,000 of the Service revenue should be withheld.

Background

2. The Tribunal has paid full regard to the material supplied by the Executive. In respect of the material submitted by the Executive, the Tribunal noted in particular:
 - a) There have been 337 complaints received about the Service from members of the public alleging that they had been signed up to the service without their consent;
 - b) The nature of the apparent breaches referred to by the Executive, namely that the service had been inappropriately marketed to consumers via the use of "content locking" and that consumers had been treated unfairly and inequitably as the incentives offered to consumers, specifically "virtual currency", had not been provided.;
 - c) Despite repeated requests by the Executive for financial information in the form of bank statements, the Level 2 provider had failed to supply such information;
 - d) The information in the Track 2 Withhold Assessment.
 - e) The Level 2 provider's written response to the Application.
3. The Tribunal has paid regard to paragraphs 4.5.1 (b), 4.6.1 - 4.6.5 of the Code and the Supporting Procedures, including the factors set out at paragraph 80 and paragraph 91 of the Supporting Procedures.

4. The Tribunal notes that the burden of proof remains on the Executive throughout and that it is for the Executive to satisfy the Tribunal that the grounds for the application are made out, and in particular that the Level 2 provider cannot or will not comply with any financial sanction that may subsequently be imposed by a Tribunal in due course.
5. Having considered the evidence before it, the Tribunal has made the following determinations:
 - a) At first appearance (and subject to evidence, arguments or information being later supplied and/or tested), there is prima facie evidence that breaches of rules 2.5.6 and 2.3.1 of the Code have occurred.
 - b) In reaching this decision, the Tribunal has considered the representations of both the Executive and the Level 2 provider. The Tribunal considers that there is clear evidence to support a prima facie breach of rule 2.5.6 of the Code in the form of the Executive's monitoring report in respect of the Service. This report captures the use of "content locking" in the promotion of the Service. In addition, the Level 2 provider acknowledges in its response that "content locking" did occur. The Tribunal notes the Level 2 provider's submission that the "content locking" was brought about by the actions of a marketing agency with whom it had contracted to market the service, and that the Level 2 provider had contractual measures in place to prohibit this type of activity. However, the Tribunal's view is that Level 2 provider remains responsible for the promotion of its services at all times which includes ensuring that the relevant agent's monitoring procedures comply with the requirements of the Code at all times. The fact that affiliate marketers may have engaged in inappropriate marketing practices without the knowledge of the Level 2 provider does not absolve the Level 2 providers of its responsibility under the Code. This responsibility is made clear in the PSA's published Guidance on Digital Marketing.
 - c) The Tribunal is also satisfied that there is evidence to support a prima facie case that a breach of rule 2.3.1 of the Code has occurred. The Executive submits that consumers were induced into entering the Service by the promise of virtual currency which was not in fact delivered to consumers. The Level 2 provider states in its response that this was due to the actions of affiliate marketers and that all subscribers must be provided the currency promised. The Executive has reviewed the material supplied by the Level 2 provider, but it is not satisfied that the information supplied to consumers was for the benefit of consumers, or that the information supplied was sufficient to fulfill the promise of virtual currency. The Tribunal agrees with the Executive's view, based upon the available evidence. The

Tribunal is satisfied that the currently available evidence is sufficient to establish a prima facie case that a breach has occurred.

- d) The Tribunal is *not satisfied* on the evidence before it that the Level 2 provider will be **unable** to pay such refunds, administrative charges and/or financial penalties that may be imposed by a Tribunal in due course. Although the Tribunal has some concerns regarding the Level 2 provider's ability to pay, due to the lack of evidence of currently available funds, these concerns are not sufficient to establish that the Level 2 provider will be unable to pay.
- e) The Tribunal notes in particular:
 - i) The latest accounts show monies of approximately £200,000 with no overdraft available
 - ii) The Level 2 provider has supplied evidence of monies received but not monies now available
 - iii) The Level 2 provider failed to supply bank statements when requested to do so
- f) The Tribunal is satisfied that the Level 2 provider will be unwilling to pay such refunds, administrative charges and/or financial penalties that may be imposed by a Tribunal in due course. The Tribunal notes in particular that:
- g) The Level 2 provider failed to fully co-operate with the Executive in supplying the financial information requested by failing to supply bank statements.
- h) The Level 2 provider was asked to supply the bank statements in October 2017 and again in November 2017 but failed to do so.
- i) The Executive's application for interim measures made it clear that the bank statements were still required but, despite this, the Level 2 provider again failed to provide the requested information.
- j) The Tribunal does not consider the Level 2 provider's representations, namely that the information requested is commercially sensitive and that the Executive does not need the information, to be adequate reasons for the non-provision of the information. In addition, the Level 2 provider's representations demonstrate that the Level 2 provider made a choice not to supply the requested information and that this was not an inadvertent oversight on its part.

- k) The repeated failure of the Level 2 provider to supply the requested bank statements gives rise to real concerns that the Level 2 provider will also be unwilling to comply with any financial sanction that may be imposed by a Tribunal in due course.
- l) The Tribunal notes that, on the face of the evidence, the Level 2 provider has made refunds to consumers to an extent, and this does provide some evidence that the Level 2 provider would be willing to comply with any sanctions subsequently imposed.
- m) However, the Tribunal's overall assessment is that the evidence in the round is sufficient to satisfy the Tribunal on the balance of probabilities that the Level 2 provider will be unwilling to co-operate in paying any financial sanctions which may be imposed in due course
- n) The Tribunal has considered the Executive's assessment of the likely future final sanctions, together with the 327 complaints generated by the Service to date, the gross Level 2 provider revenue of £447,391 and the estimated revenue flowing from the apparent breaches of £24,640 which the Executive has estimated by calculating a figure for average consumer spend.
- o) The Tribunal considers that a Tribunal at the substantive hearing of this matter would likely view the apparent breaches of the Code as very serious and impose a fine in the region of £100,000 and a general refund sanction, in order to achieve the sanctioning objective of removing the financial benefit and achieving credible deterrence.
- p) In reaching this determination the Tribunal has considered the Level 2 provider's submissions that the Executive's assessment of likely sanctions is disproportionate considering the Level 2 provider's level of co-operation, the refunds made to consumers, the fact that affiliate agencies were contracted on a proper basis and the fact that Empello was engaged to carry out due diligence. The Tribunal considers that these measures do not affect the Level 2 provider's responsibilities under the Code.
- q) The Tribunal has also considered the Level 2 provider's submission that 327 complaints is a small percentage when measured against the subscriber base. On this specific point, the Tribunal is aware that only a small percentage of consumer complaints reach the PSA and therefore does not find this submission persuasive.

- r) The Tribunal therefore considers that the measures set out below are necessary and proportionate to take in the circumstances of this case. In assessing the potential impact of the measures on the Level 2 provider, the Tribunal takes into account the Level 2 provider's submission that any withhold of service revenue will affect its business volume and cause real damage, although it is noted that no specific information is given about how the Level 2 provider proposes to expand its existing services. It is noted by the Tribunal that the Level 2 provider's submissions appear to be addressing sanctions at final stage, rather than a withhold of revenue at interim stage. The Tribunal is satisfied that the potential impact on the Level 2 provider is proportionate and justified, when balanced against the very serious nature of the apparent breaches, the resulting consumer harm and the need to achieve the sanctioning objectives.
 - s) The Tribunal also agrees with the estimated future administrative costs of £15,000.
6. Accordingly, in respect of the Service the Tribunal hereby directs that:
- a) The PSA is authorised to direct a withhold of up to £115,000;
 - b) The sums directed to be withheld may be allocated and re-allocated between any Network operators or Level 1 providers for the Service as the Executive sees fit from time to time, provided that the total sum withheld by all providers does not exceed the maximum sum authorised in this decision.
 - c) The Executive is given discretion to vary the total directed to be withheld downwards in the event that it is provided with alternative security which is, in its view, sufficient to ensure that such refunds, administrative charges and/or financial penalties as it estimates a CAT may impose in due course are paid.
 - d) Such interim measures are to be revoked upon the case being re-allocated to Track 1 or otherwise discontinued without sanction

Mohammed Khamisa QC
Tribunal Chair
19.09.2018

Application for review of interim measures pursuant to Code of Practice paragraph 4.6.6

Case reference: 134234
Level 2 provider: Net Real Solutions, S.L.
Type of service: Multi-media subscription service
Service name: Appicateka
Network operator: all mobile network operators

This is an application by Net Real Solution, S.R. (the "**Applicant**") for a review of an interim measure imposed on 19 September 2018, namely a direction that up to £115,000 of the Service revenue should be withheld.

Background

1. On 19 September 2018 a previous Tribunal directed that the Phone Paid Services Authority (the "PSA") was authorised to direct a withhold of service revenue of up to £115,000, following an application by the PSA's Executive pursuant to paragraph 4.6 of the Code.
2. On 5 October 2018 the Applicant submitted an application for a review of the decision of the previous Tribunal.
3. On 22 October 2018 a differently constituted Tribunal of the Code Adjudication Panel ("CAP") considered the application for review, in accordance with paragraph 4.6.6. (a) of the Code.
4. The Tribunal paid full regard to the material supplied by the parties, including:
 - the previous adjudication of the Tribunal, whereby interim measures were imposed dated 19 September 2018
 - the application for review and supporting documentation dated 5 October 2018.

Adjudication

5. The Tribunal has paid regard to the requirements of paragraph 4.6.6. (a) (ii) of the Code.
6. It is asserted by the Applicant that the following material amounts to new information for the purposes of paragraph 4.6.6 (a) (ii) of the Code:

- 2017 Annual Accounts of the Applicant
- 2017 Audit Report of the Applicant

7. The Applicant asserts that this information was not previously disclosed to the PSA as it had previously considered that all documentation and information available and necessary for the study of the case, related to the Applicant's business in the UK, had been provided. The Applicant states that it now understands that the additional information now supplied is relevant and that it needs to be considered by the Tribunal in its decision making.

8. The Tribunal notes that the information now supplied was available to the Applicant as of January 2018 and was therefore available at the time of the original interim measures hearing. The Applicant chose not to supply it initially, for the reasons outlined in the application.

9. The Tribunal accepts that the additional financial information provided is new information for the purposes of paragraph 4.6.6. (a) (ii) of the Code.

10. The Tribunal does not however accept that the contents of Part 1 of the Applicant's application is new information, as this material amounts to an argument against the original decision of the Tribunal and is a simple re-iteration of the points made to that previous Tribunal. The Tribunal notes that the scope of this review of interim measures, for the purposes of paragraph 4.6.6 (a) (ii) of the Code, is to determine whether new information has come to light, suggesting that the application of interim measures was not or is no longer appropriate. Paragraph 4.6.6 (a) (ii) does not permit a re-hearing of the original decision.

11. The Tribunal therefore turns its mind to consider whether, on a balance of probabilities, the new information supplied by the Applicant in the form of 2017 annual accounts and a 2017 audit report, is sufficient to establish that the application of interim measures by the previous Tribunal was not, or is no longer appropriate.

12. Whilst the Tribunal accepts that the annual accounts and audit report are new information, it is of note that this information was only supplied after the withhold of service revenue was imposed. It is also of concern that the Applicant has failed to provide bank statements, despite repeatedly requested by the Executive for the same, and despite the previous Tribunal indicating that the failure to supply this information amounted to evidence of a lack of co-operation by the Applicant.

13. The Applicant asserts that it is willing to comply with any financial sanctions that may be imposed by a Tribunal in due course and details the steps it has taken in order to fully co-operate with PSA. The Tribunal has carefully considered the representations of the Applicant in this regard.

14. Notwithstanding the Applicant's submission that it is willing fully co-operate with the Executive and comply with any sanctions that may be imposed, for the following reasons we do not have confidence that the Applicant will do so:

i. The Applicant has not still not supplied the bank statements requested by the Executive, which was also a relevant factor in the original Tribunal's finding that the Applicant would be likely to be unwilling to pay any future financial sanction. The Tribunal considers that the Applicant has failed to advance any good reason for its continuing failure to supply the information requested.

ii. If Audited accounts and Audit report had been supplied at the previous hearing, our finding is that it would not have altered the decision of the original Tribunal in light of the continued failure by the Applicant to supply bank statements.

iii. The submissions made by the Applicant at page 12 of the application for review, specifically that *"my client would be willing to be fully co-operate with PSA but, independently, said sanction must be based on demonstrated responsibility which, in this case, we consider that it has not been sufficiently proven based on the exposed arguments"*. This Tribunal's view is that this is a qualified agreement to co-operate, which is conditional upon the Applicant agreeing with the finding of any subsequent Tribunal. This qualified agreement to co-operate supports the grounds for a withhold of service revenue rather than undermines it, as it suggests that the Applicant will only be willing to comply with any future sanctions if it agrees with the reasoning and findings of the Tribunal.

15. The evidence in the round and in particular the continuing failure by the Applicant to supply bank statements or to state an unqualified willingness to co-operate indicates that the Applicant will not be unwilling to comply with any financial sanctions that may be imposed. The additional financial evidence supplied by the Applicant does not significantly alter the evidential position and there has not been a change in circumstances since the original hearing.

16. For the reasons set out above, the Tribunal is satisfied on a balance of probabilities that the Applicant will not be willing to comply with any financial sanctions that may be imposed by a Tribunal in due course.

17. Accordingly, the test in paragraph 4.6.6. of the Code is not made out. The determination of the Tribunal is that the interim measures are necessary and proportionate and that they should continue pending completion of the investigation of the case.

Ian Walden
Tribunal Chair
29 October 2018

