Adjudicator's Report

Wireless Application Service Providers' Association

Complaint number	30975
Cited WASPA members	Takeo Limited (1614)
Notifiable WASPA members	Opera Telecom (Proprietary) Limited (0068)
Source of the complaint	WASPA Media Monitor
Complaint short description	A subscription service where subscriptions are facilitated by means that circumvent established double opt-in requirements.
Date complaint lodged	2016-07-08
Date of alleged breach	The date of the alleged breach (if known).
Applicable version of the Code	14.4
Clauses of the Code cited	4.2, 5.4, 5.5, 8.2, 8.8, 12.1, 12.2, 15.9, 15.10 (i, ii and iii)
Related complaints considered	None.
Fines imposed	A fine in the amount of R100 000 in respect of the member's breaches of sections 4.2, 5.4, 5.5, 15.9 and 15.10 of the Code; and A fine in the amount of R50 000 in respect of the member's breaches of sections 8.2, 12.1 and 12.2 of the Code.
Is this report notable?	Notable

Summary of notability	This complaint highlights a technically advanced mechanism for circumventing established safeguards to ensure informed, double opt-in subscription mechanisms. The underlying mechanisms are highly deceptive and seemingly designed intentionally in this manner.

Initial complaint

This complaint involves a degree of technical complexity. At its essence, it pertains to a subscription service operated by the member ("the service") that the Monitor identified as being in breach of various provisions of the Code.

The Monitor tested the service and documented both its testing methodology and findings in an annexure to its complaint. I have attached that annexure to this report and marked it "A". The Monitor's testing process is relatively technical. The manner in which the test was documented offers a view of what the Monitor actually saw and experienced along with documentation of the underlying processes.

In short, the service is called Phonegenie. It involves offers of adult content and is triggered by clicking on a banner ad. The end result of a somewhat convoluted process is that a consumer is subscribed to the service and receives a subscription confirmation message.

This complaint focuses on what precedes this notification and the fact of the consumer's subscription.

The Monitor's concern is that the service somehow circumvents the double opt-in process prescribed by the Code. How the service accomplishes this is not clear. The Monitor identified two possible methods of technical subterfuge that trick the consumer into subscribing unwittingly. The member contended that there was a technical flaw in the process and this led to a subscription that bypassed the requisite double opt-in process.

The complaint was initially directed at Opera Telecom. Opera Telecom's response to WASPA indicated that it had suspended the member and queried the rationale for an emergency procedure the Secretariat invoked in response to the complaint.

After some correspondence, the Secretariat withdrew the complaint against Opera Telecom and lodged it against the member as the party it regarded as the appropriate respondent.

Member's response

The member responded to the complaint on 2016-07-25 with two attachments, which are attached to this report and marked "**B1**" and "**B2**", respectively:

- The first is an email addressed to its customer, Reach Effect, dated 2016-06-14 (before the complaint was lodged) advising Reach Effect that the member had taken note of apparently non-compliant campaigns and was terminating the relevant campaigns.
- The second was a specific response to the complaint that seemed to focus more on specifics of the testing process than the substantive aspects of the complaint itself.

In the second document, the member advised the Secretariat as follows:

> *Because our affiliate (reacheffect) is claiming that they experienced an isolated technical failure, we present this to you now to pass their claim it was an isolated incident and that this issue had not affected multiple users.*
>
> *That being said, we had already taken action to cut all ties with the affiliate. We experienced non-compliant banners from the same affiliate just the day prior to this test and as a result we terminated our relationship (see attached). The test took place at 02:00 and the affiliate traffic was stopped only a few hours later. We withheld payment and are no longer involved with them whatsoever and no longer have affiliates working on the service.*

Request for clarification

Certain aspects of the matter were unclear to me. I prepared questions for the member and the Monitor in terms of clause 24.31 and requested further information from both parties. I am grateful to both the member and the Monitor for their further submissions.

Member's further response

The member's responses and my questions are below:

> *Dear WASPA, please see the following answers below in red:*
>
> *1. In the first part of your response to the WASPA Secretariat dated 2016-07-20, you indicated that the apparent page load delays (for example, between time references 01:27 and 03:28) are due to "technical failures" which were interpreted to lead to a "loop that resulted in a malfunction".*

1.1. Please clarify the nature of these technical failures?

TAKEO: The source of the failure is unknown as it appeared, from the video provided, to be an issue with the users phone, 3G service, or browser. We can recognize this by the presence of the spinning wait cursor in the video provided and the log lag times in processing the page(s).

1.2. Please advise whether the Monitor's device would have called/loaded any pages other than the pages which were rendered in the video? If so, please list the relevant pages and describe their functions?

TAKEO: We see the tester had attempted to load (or did load) the page while the video was not recording. We know this because the video shows pages included in the browser window with our landing page.How do we know what happened there while the video was not running? All actions performed on our pages should have been kept in the recording for purposes of full disclosure.

2. In the second part of your response to the WASPA Secretariat, you suggested "there may have been some actions that also lead to the final subscription taking place".

TAKEO: It's possible the user performed actions that we are unaware of when portions of testers on page interactions are missing from the recording. How do we know what happened when the video is shut off and turned back on? Anything could have happened and it doesn't make sense to leave that out of the video.

2.1. Please list and describe what the process ought to have been in the absence of the "technical failures" you described in the first part of your response to the WASPA Secretariat? What should the Monitor have seen and which steps ought the Monitor to have taken to confirm a subscription to the service?

TAKEO: Pages should load rapidly and carrying users through a smooth and clear page flow.

2.2. Please advise to what extent Reach Effect's campaign was compliant with the WASPA Code's requirements?

TAKEO: Other than the issues noted in this document, all actions were compliant with WASPA code of conduct.

2.3. Please advise what steps you took to ensure that the Reach Effect campaign was compliant with the WASPA Code at all times?

TAKEO: We perform daily tests of the service with rotating devises.

2.4. Please explain how the Monitor received a welcome message as described in the test and clarify what triggered this welcome message?

TAKEO: We aren't clear on this, only a carrier page can trigger a subscription, which is why we suspect a technical issue.

2.5. Please clarify whether receipt of the welcome message confirms successful subscription to the relevant service?

TAKEO: Yes it does.

2.6. Please advise how long this particular service with its subscription mechanisms and campaign elements remained operational and available to the public prior to its suspension?

TAKEO: Reach Effect's operations were ceased as noted 2016-06-10.

2.7. Your email to Reach Effect regarding a specific "explicit banner" is dated 2016-06-10. Please advise when you first became aware of a problem with the service?

TAKEO: As soon as notified from WASPA, but we had ceased operations prior to that notification.

Complainant's further response

The Monitor's further submissions were comprehensive. I have attached them and marked them "**C**".

Sections of the Code considered

Version 14.4 of the Code applies to this complaint. The Monitor cited the following provisions of the Code:

Professional conduct

4.2. Members must at all times conduct themselves in a professional manner in their dealings with the public, customers, other service providers and WASPA.

…

Provision of information to customers

5.4. Members must have honest and fair dealings with their customers.

5.5. Members must not knowingly disseminate information that is false or deceptive, or that is likely to mislead by inaccuracy, ambiguity, exaggeration or omission.

…

8. Advertising in general

Definition of pricing information

8.1. …

*8.2. For a subscription service, the "**pricing information**" consists of the word "**subscription**" and the cost to the customer and frequency of the billing for the service. The cost and frequency portion of the pricing information must follow the following format, with no abbreviations allowed: "**RX/day**", "**RX/week**", or "**RX/month**" (or RX.XX if the price includes cents). For services billed at an interval other than daily, weekly or monthly, the required format is "**RX every [time period]**", with no abbreviations permitted when specifying the time period. Examples of pricing information: "**Subscription R5/week**", "**R1.50/day subscription**", "**RX every three days**", "**RX every two weeks**".*

…

12. Web advertising

Display of pricing information

12.1. For any web page, pricing information does not need to be displayed for services which are free, or which are billed at standard rates. For all other services, where there is a call-to-action, pricing information must be clearly and prominently displayed immediately adjacent to the call-to-action.

12.2. There must not be any intervening text or images between the call-to-action and the pricing information. Pricing information must be legible, horizontal and presented in a way that does not require close examination. Pricing information must not be obscured by any other information. Pricing information must not be animated. It must not be a requirement that the viewer of an advert has additional software installed in order to see pricing information in the advert.

…

15.9. The confirmation step for any subscription service must require an explicit response from the customer of that service. The confirmation step may not be performed in an automated manner in such a way that the process is hidden from the customer.

…

Subscriptions initiated via a web page

15.10. For all subscription services initiated via a web page, there must be an additional specific confirmation step before the customer is billed. This confirmation step must be provided in one of three ways:

(i) The customer's mobile carrier may implement the confirmation step.

(ii) The member can provide the customer with a "confirmation page".

(iii) The member can send a "confirmation message" to the customer. The customer must not be charged for the confirmation message.

Discussion

I read through the various submissions and responses to my additional questions. I have no reason to doubt the Monitor's description of its tests. I am comfortable the Monitor captured the tester's full experience which would have been shared by a user under comparable circumstances. Flowing from this, the Monitor's test reveals the following:

1. A number of redirects occurred which loaded various mobile pages automatically after the Monitor clicked on a banner ad and, subsequently, an initial call to action button.
2. The content offered on various pages which were presented to the Monitor were not consistent:
    2.1. The initial landing page offered adult content under the banner "Wetplace". The call to action button on this landing page made no reference to any age limits, subscription services and pricing or terms and conditions that may govern access to such content.
    2.2. A subsequent page offered "Power Management features" through the Phonegenie service. There was no pricing information presented on this particular page, only small text at the bottom of the screen reiterating an offer of software to improve Android phone performance.
    2.3. A welcome message that appears to have been triggered by the Monitor tapping on the Phonegenie call to action offered access to "the best apps for your Android" with the first mention of the subscription cost of R5/day.
3. At no point was a network-hosted confirmation page displayed to the Monitor to afford the Monitor an opportunity to complete the double opt-in subscription process and trigger both the subscription itself and authorise payments.

4. The Monitor's phone was, in fact, subscribed to the service and this is evidenced by the welcome message. This is accepted by both the member and the Monitor.

Whether the subscription was facilitated by clickjacking or a Javascript Same Origin Bypass is unclear and largely irrelevant to the outcome. The member contended that the Monitor was subscribed due to a technical fault but failed to adduce any substantive evidence that such a fault was the proximate cause of the subscription.

I find the Monitor's response[1] to the member's suggestion of a technical failure to be persuasive:

If there was a technical failure or glitch, as alleged by the member, then the procedure should have ended with the faulty service landing page, not activated a subscription service without the required procedure being voluntarily completed by the tester.

Even if I accept the member's argument that there was a technical failure and not an intentional circumvention of the required subscription mechanism, I must find that the manner in which the technical failure manifested is highly problematic.

What the member's explanation of a technical fault means is that the fault would still have triggered a subscription through the network-hosted confirmation page. Bear in mind that the network-hosted confirmation page is not under the member's (or its affiliates') control and so the member's system would have had to trigger the subscription mechanism through the network-hosted confirmation page independently of the Monitor's volition.

In other words, the effect of this alleged technical fault is functionally indistinguishable from an intentional subterfuge.

Functionally, I see no difference between an intention subterfuge in the form of clickjacking or a Javascript Same Origin Bypass and a technical fault resolution mechanism that still triggers a subscription instead of simply reporting a fault in some manner intelligible to a user in the Monitor's position.

The only conclusion I can reasonably draw is that the service was engineered to trigger a subscription without following the prescribed double opt-in process.

The service is deceptive and seemingly designed to facilitate an involuntary subscription to a service that is likely not what it appears to be. The lure is an adult content service that lacks any indication of the mandatory "18+" advisory, subscription nature of the service, subscription pricing and required terms and conditions.

---

[1] At page 3 of the Mon tor's further subm ss ons n response to my quest ons

The actual subscription service appears to be be the Phonegenie Android app subscription service which is similarly not presented using a subscription mechanism that meets the Code's notice requirements.

Decision

In light of my findings above, I find that the service is in breach of sections 5.4, 5.5, 8.2, 12.1, 12.2, 15.9 and 15.10. Furthermore, I am concerned that the member sought to justify the highly problematic subscription to the service as a technical fault without a reasonable explanation for how such a fault could have such a result.

The member's conduct in presenting this deceptive service that flagrantly circumvents the safeguards put in place to prevent involuntary and uninformed subscriptions is worrying. I am also concerned that the member failed to conduct a reasonable investigation into the service's functionality and ensure its compliance with the Code. Accordingly, I find that the member has not conducted itself in a professional manner as envisaged by section 4.2 of the Code.

Sanctions

Flowing from my findings above, I recommend the following sanctions against the member:

- A fine in the amount of R100 000 in respect of the member's breaches of sections 4.2, 5.4, 5.5, 15.9 and 15.10 of the Code; and
- A fine in the amount of R50 000 in respect of the member's breaches of sections 8.2, 12.1 and 12.2 of the Code.

These fines are payable on demand by the Secretariat.

Matters referred back to WASPA

This service points to a possible use of highly deceptive practices by certain members and highlights the importance of the sort of in depth testing the Monitor conducted in this matter. Without the Monitor's more detailed and technical testing, such deception may not have been as apparent. I recommend that such detailed testing continue and adapt to new technical challenges presented by unscrupulous members.

POTENTIAL FRAUDULENT ACTIVITY – CASE #2

2016.06.14_02:00_OXYGEN8_PHONEGENIE

DETAILS:

REFERENCE: 2016.06.14_02:00_OXYGEN8_PHONEGENIE
DATE: 14 June 2016
TIME OF TEST: 02:00
NETWORK: MTN
MSISDN: [redacted]
AIRTIME BALANCE BEFORE: R 496.00
AIRTIME BALANCE AFTER: Not displayed in test
AGGREGATOR INVOLVED: Oxygen8
SERVICE NAME: Phonegenie Subscription Service
SHORT CODE: 37914

NOTES:

Recordable.mobi:

- Software used to record the activities, audio, visuals and gesture rendering on a mobile device in video format.
- The tester activates this software on the mobile device used to test services in order to ensure that we capture the tester's exact actions in an indisputable manner.
- The video will display the journey the tester takes to illustrate what consumers factually experience whilst browsing on the internet and interacting with specific services.
- More importantly, the video will serve as concrete evidence of what the tester actually sees and the actions the tester explicitly takes.
- The video will therefore showcase whether due procedure was followed, or alternatively where the required procedure does not take place, is by-passed or automated.

PacketCapture:

- Software used to intercept and log traffic that passes over a digital network or part of a network. As data streams flow across the network, the software captures each packet and, if needed, decodes the packet's raw data, showing the values of various fields in the packet, and analyses its content according to the appropriate specifications.

- The tester activates this software on the mobile device used to test the services in order to capture network traffic - the interaction between the mobile handset, various websites, advertisements, the service, and if applicable, the mobile network operator's systems and servers.
- The data will provide evidence to show whether the mobile handset (associated with a specific MSISDN) interacted with the mobile network operator's system to log a requests to join the subscription service, and the subsequent approval granted by the network to the aggregator to bill the user.
- In order to access the PacketCapture data provided, the following program needs to be downloaded to review the data: 'Wireshark' available at https://www.wireshark.org/.

REQUIRED PROCEDURES AND POSSIBLE FRAUDULENT ACTIVITY:

- Required Procedure Flow 1: The user will browse on the internet and click on a banner advertisement promoting the subscription service. The user will be directed to the service landing page, which needs to contain certain terms and conditions. Once a user clicks on the call to action button on the service landing page, the final confirmation step is triggered and the network hosted confirmation page is displayed. Only when a user actively clicks on the 'Accept' (or similar) button on the network hosted confirmation page, will the MNO provide authorisation for the service to be activated and the aggregator will receive permission to bill the user accordingly. The user receives a welcome message to confirm that the subscription has been activated.
- Required Procedure Flow 2: The user will browse on the internet and click on a banner advertisement promoting the subscription service, which needs to contain certain terms and conditions. This will trigger the final confirmation step and the network hosted confirmation page is displayed. Only when a user actively clicks on the 'Accept' (or similar) button on the network hosted confirmation page, will the MNO provide authorisation for the service to be activated and the aggregator will receive permission to bill the user accordingly. The user receives a welcome message to confirm that the subscription has been activated.
- Possible fraudulent activity (including, but not limited to):
    - The user clicks on a banner advertisement and gets subscribed to a service:
        - No service landing page displayed – therefore the user did not click on the call to action button to trigger the network hosted confirmation page (if flow 1 is applicable);
        - No network hosted confirmation page displayed – therefore the user did not actively click on the 'Accept' (or similar) button and did not expressly agree to join the service;

        - In some cases, the user receives a welcome message to confirm subscription to the service, other times no welcome message is received and the subscription is detected via airtime being deducted etc.
    - The user clicks on the call to action button on the service landing page and gets subscribed to a service:
        - No network hosted confirmation page displayed – therefore the user did not actively click on the 'Accept' (or similar) button and did not expressly agree to join the service;
        - In some cases, the user receives a welcome message to confirm subscription to the service, other times no welcome message is received and the subscription is detected via airtime being deducted etc.
    - The user is directed to the network hosted confirmation page (via a banner or by clicking on the call to action button on the service landing page, depending on the required flow) and gets subscribed to a service:
        - The user did not click on the 'Accept' (or similar) button and did not expressly agree to join the service;
        - The network hosted confirmation page is displayed, but a few seconds later (without any interaction by the user), the subscription is activated;
        - The active acceptance by the user (which should happen manually when the user clicks on the 'Accept' (or similar) button) does not take place and this step is automated – completed without the users express consent;
        - In some cases, the user receives a welcome message to confirm subscription to the service, other times no welcome message is received and the subscription is detected via airtime being deducted etc.

NETWORK PROCEDURES:

- In very simplified terms, once a user actively clicks on a member's promotional banner (flow 2) or the call to action button on the service landing page (flow 1), the member's system sends a request to the MNOs system.
- This interaction will entail that the member's system logs a request on the MNOs system that the MSISDN has requested to join a specific subscription service at a predetermined cost.
- This request triggers the confirmation step and the network hosted confirmation page is displayed to the user.
- The MNO is in control of this page, which notifies the user that they have requested to join a subscription service at a specified cost. The user is

prompted to either confirm or reject this request by clicking on the appropriate option – ‘Accept’ (or similar button) or ‘Decline’ (or similar button).

- If the user clicks on the ‘Decline’ button, the process ends and the subscription service is not activated.
- If the user fails to take any action or exits the procedure, the process ends and the subscription service is not activated.
- If the user clicks on the ‘Accept’ button, the MNOs system authorises the activation of the subscription service and sends an approval confirmation to the member’s system. The MNOs system furthermore provides the member’s system with permission to bill the MSISDN.

METHODS IDENTIFIED TO BY-PASS OR AUTOMATE THE NETWORK CONTROLLED PROCEDURE:

Click-Jacking:

Concept in simplified terms:

- The malicious practice of manipulating a website user's activity by concealing hyperlinks beneath legitimate clickable content, thereby causing the user to perform actions of which they are unaware.
- A click-jacked page tricks a user into performing undesired/unknown actions by clicking on a concealed link. On a click-jacked page, the attackers load another page over it in a transparent layer. The users think that they are clicking visible buttons, while they are actually performing actions on the hidden/invisible page.
- The hidden page may be an authentic page; therefore, the attackers can trick users into performing actions which the users never intended or knew about. There are limited ways of tracing such actions to the attackers later, as the users would have been genuinely authenticated on the hidden page.

Possible user experience and consequences:

- Example 1:
    - The user views a banner or article on a webpage whilst browsing on the internet. This page has been click-jacked and serves as a top layer for the hidden bottom layer which is actually the network hosted confirmation page.
    - If the user clicks on the banner or link in the article, they are in fact clicking on the ‘Accept’ (or similar) button which is contained on the bottom hidden layer.
    - This action activates the subscription service without the user’s knowledge or explicitly consent.
- Example 2:

  - The user views a banner or advertisement on a webpage whilst browsing on the internet. The user clicks on the banner or advertisement that directs the user to the service landing page.
  - This service landing page has been click-jacked and serves as a top layer for the hidden bottom layer which is actually the network hosted confirmation page.
  - If the user clicks on the call to action button on the service landing page, they are in fact clicking on the 'Accept' (or similar) button which is contained on the bottom hidden layer.
  - This action activates the subscription service without the user's knowledge or explicitly consent.
- Result:
  - The user never sees the network hosted confirmation page as this page is layered/masked/camouflaged. The user does therefore not explicitly or intentionally click on the 'Accept' (or similar) button to activate the service, however the user is subscribed to the service.
  - The user usually has no proof that the required procedure has not been followed, as it is their word against 'factual' proof in the form of logs.
- Problem:
  - The member's system has at some point whilst the user was browsing on the internet logged a request on the MNOs system that the MSISDN requested to join the subscription service.
  - The network hosted confirmation page was duly triggered, however never visibly displayed to the user, as this page has been concealed.
  - The user clicks on the 'Accept' (or similar) button without their knowledge.
  - The MNOs system receives this acceptance confirmation and sends a confirmation to the member's systems that authorises the activation of the subscription service and permission to bill the user.
- Conclusion:
  - The user will deny subscribing to the subscription service and will allege that they never saw the network hosted confirmation page and did not expressly consent to join the service by clicking on the 'Accept' button.
  - The member will be able to provide company logs to prove interaction with the member's service as well as network logs to prove acceptance of the service on the network hosted confirmation page via the authorisation sent by the MNOs system to the member's system.
  - This acceptance however happened in the background without the user's knowledge due to the MNOs confirmation step being compromised by being by-passed and/or automated.

JavaScript Same Origin Bypass:

Concept in simplified terms:

- Same Origin Policy (SOP) is a security measure used in web browser programming languages such as JavaScript and Ajax to protect the confidentiality and integrity of information. SOP prevents a web site's scripts from accessing and interacting with scripts used on other sites.
- The essence of the SOP can be formulated as: windows can work in contexts of each other only if they are from the same protocol://domain:port, or, shortly, from the same origin.
- Resources with the same origin have full access to each other. If pages A and B share the same origin, JavaScript code included on A can perform HTTP requests to B's server, manipulate the DOM of B or even read cookies set by B. If they are not the same origin, SOP restricts this activity.
- By by-passing JavaScript SOP, malicious script from another site could interact with a script from a legitimate site without restriction, potentially leading to data being compromised.

Possible user experience and consequences:

- Example 1:
    - The user views a banner on a webpage whilst browsing on the internet and clicks on the banner which triggers the confirmation step.
    - The network hosted confirmation page is however opened in another browser window and bypasses the SOP.
    - By bypassing the SOP, the attacker would then be able to access DOM elements within the network hosted confirmation page, and manipulate the script to automatically trigger the acceptance procedure on the page.
    - This action activates the subscription service without the user actively clicking on the 'Accept' (or similar) button.
- Example 2:
    - The user views a banner on a webpage whilst browsing on the internet and clicks on the banner which redirects the user to the service landing page.
    - The user clicks on the call to action button on the service landing page, which triggers the confirmation step.
    - The network hosted confirmation page is however opened in another browser window and bypasses the SOP.
    - By bypassing the SOP, the attacker would then be able to access DOM elements within the network hosted confirmation page, and manipulate the script to automatically trigger the acceptance procedure on the page.
    - This action activates the subscription service without the user actively clicking on the 'Accept' (or similar) button.

- Result:
    - The network hosted confirmation page is displayed to the user - note that the page is actually shown to the user, as opposed to the Click-Jacking case, where it is hidden.
    - Due to the bypassing of the SOP, the attacker automates the acceptance of the subscription to the service.
    - There is not any human interaction with the network hosted confirmation page – the user does not actively click on any button contained on the network hosted confirmation page.
- Problem:
    - The member's system correctly logged a request on the MNOs system that the MSISDN requested to join the subscription service.
    - The network hosted confirmation page was duly triggered and displayed to the user, however it was opened in another browser to bypass the SOP security measure which enabled malicious script from another site to interact with a script from the legitimate network hosted confirmation page without restriction.
    - This triggered an automated acceptance of the subscription to the service, without any actually action taken by the user.
    - The MNOs system receives this acceptance confirmation and sends a confirmation to the member's systems that authorises the activation of the subscription service and permission to bill the user.
- Conclusion:
    - The user will deny subscribing to the subscription service and will allege that they did not expressly consent to join the service as they never clicked on the 'Accept' button.
    - The member will be able to provide company logs to prove interaction with the member's service as well as network logs to prove acceptance of the service on the network hosted confirmation page via the authorisation sent by the MNOs system to the member's system.
    - This acceptance was however automated with no action taken by the user. The MNOs confirmation step was compromised by being by-passed and/or automated.

TEST RESULT:

Video evidence:

Kindly find a link to the video here: [redacted]

(Note: the timeline has been included for ease of reference – please make provision for minor differences compared to actual video timeline due to manual capturing)

- (00:00) – Enabled PacketCapture software;
- (00:01) - Switched on Recordalbe.mobi software;
- (00:03) - Checked starting airtime balance on MTN network;
- (00:15) - Selected Internet application;
- (00:22) - Entered 'wetplace.com' in the address bar and directed to site;
- (00:35) - Browed on 'm.wetplace.com';
- (00:40) - Scrolled on the site and clicked on the second video image;
- (00:45) – Redirect to 'm.wetplace.com':
    - Second browser window/tab opened;
- (00:48) – Scrolled on the site and clicked on the first video image;
- (00:50) – Redirect to 'm.wetplace.com':
    - Third browser window/tab opened;
- (00:52 – 01:09) – Scrolled on the site and clicked on a video;
- (01:09) – Redirect to 'main.exoclick.com':
    - Fourth browser tab opened;
- (01:10 – 01:17) – Scrolled on the site:
    - Note: did not click on any image or video displayed;
- (01:18) – Whilst browsing on the site, the tester was automatically redirected (URL changed):
    - URL in address bar: 'batesk.com/landing';
- (01:19) – The tester swiped the screen to remove/minimise the fourth browser window/tab to display the browser window/tab beneath it (third browser tab);
- (01:21) – The tester swiped the screen to remove/minimise the third browser window/tab to display the browser window/tab beneath it (second browser tab);
- (01:22) – The 'Phonegenie' subscription service landing page was displayed:
    - Green 'Continue' call to action button visible;
    - The service landing page is non-compliant:
        - Subscription reference not immediately adjacent to the call to action button;
        - Pricing and billing frequency not immediately adjacent to the call to action button;

        - Terms and conditions displayed at the bottom of the page (too many line spacing between call to action button and terms and conditions);
        - This landing page opened in the background – tester did not click on a banner related to this service;
        - If a banner directed to this service, it was an adult banner directing to a non-adult service.
- (01:26) – Clicked on the green ‘Continue’ call to action button:
    - Note: the moment the call to action button is clicked, the terms and conditions at the bottom of the page disappears.
- (01:27 – 03:28) – Clicking on the call to action button should trigger the confirmation step and the network hosted confirmation page should be displayed to the user in order for the user to accept or decline joining the subscription service:
    - The tester was not redirected to the network hosted confirmation page;
    - The service landing page just buffers for a prolonged time.
- (03:29) – The tester clicks in the middle of the buffering service landing page;
- (03:30 – 03:32) – Redirected to a blank page:
    - Extremely small, almost illegible button at the top of the page ‘Continue’;
    - The average consumer would never have seen this – only visible when video is played in slow motion;
    - Disappears almost immediately;
- (03:33) – Tester is automatically redirected to a blank page:
    - URL in address bar: ‘track.reacheffect.com’;
    - Opens in the same (second) browser window/tab;
- (03:34) – Tester is automatically redirected to a new page:
    - URL in address bar: ‘za.phonegenie.co/p/v…’;
    - Opens in the same (second) browser window/tab;
    - States: ‘Scanning’;
- (03:35) – Page states: Scanning – Analyzing;
- (03:37) – Page states: Scanning – Device detected;
- (03:42) – Tester automatically redirected to Phonegenie service landing page:
    - The service landing page is non-compliant:
        - Subscription reference not immediately adjacent to the call to action button;
        - Pricing and billing frequency not immediately adjacent to the call to action button;
        - Terms and conditions displayed at the bottom of the page (too many line spacing between call to action button and terms and conditions);
        - If a banner directed to this service, it was an adult banner directing to a non-adult service.
- (03:46) – Tester clicks in the middle of the service landing page:

    - Note: tester did not click on the green ‘Continue’ call to action button;
- (03:47) – Redirected to ‘za.phonegenie.co/p/…’ in the same (second) browser window/tab;
- (03:47) – Automatically redirected to ‘track.reacheffect.com’ in the same (second) browser window tab;
- (03:50) - Redirected to ‘za.phonegenie.co/p/…’ in the same (second) browser window/tab;
- (03:51) – Page states: Scanning – Analyzing;
- (03:53) – Page states: Scanning – Device detected;
- (03:54) – Tester clicks on the tab/window manager;
- (03:55) – Two browser tabs are displayed:
    - 1. Phonegenie page stating ‘Analyzing’;
    - 2. Phonegenie page stating ‘Device detected’.
- (03:56) – Tester closed the second browser tab and selected the remaining browsing tab to open;
- (03:57) – Tester redirected to Phonegenie service landing page:
    - The service landing page is non-compliant:
        - Subscription reference not immediately adjacent to the call to action button;
        - Pricing and billing frequency not immediately adjacent to the call to action button;
        - Terms and conditions displayed at the bottom of the page (too many line spacing between call to action button and terms and conditions);
        - If a banner directed to this service, it was an adult banner directing to a non-adult service.
- (04:06) – Tester clicked on the green ‘Continue’ call to action button:
    - Note: the moment the call to action button is clicked, the terms and conditions at the bottom of the page disappears.
- (04:07 – 04:13) - Clicking on the call to action button should trigger the confirmation step and the network hosted confirmation page should be displayed to the user in order for the user to accept or decline joining the subscription service:
    - The tester was not redirected to the network hosted confirmation page;
    - The service landing page just buffers for a prolonged time.
- (04:13) – A SMS notification appears on the top of the phone screen;
- (04:14) – The tester minimised the buffering landing page to review the notification task pane, which included the new Welcome Message;
- (04:22) – The tester maximised the buffering landing page to review the progress:
    - Page still buffering;
    - Not redirected to any other page yet.

- (04:37) - The tester minimised the buffering landing page to review the notification task pane;
- (04:40) – The tester selected the SMS notification in the notification task pane to review the content thereof;
- (04:41) – Welcome message confirming subscription to Phonegenie at R5/day;
- (04:59) - The tester maximised the buffering landing page to review the progress:
    - Page still buffering;
    - Not redirected to any other page yet.
- (05:02) – Tester closes the buffering landing page in tab/window manager;
- (05:05) – Tester disables Packetcapture software;
- (05:07) – Tester disables Recorable.mobi software;
- (05:08) – Test concluded

TEST RESULT CONCLUSION:

On or about the 14th of June 2016 at about 02:00 the user visited the wetplace.com adult content website. The user clicked on a banner advertisement hosted at the wetplace.com site {00:40}. Note that this banner was the one that has relevance to the second browser window/tab which later on displayed the Phonegenie sevice landing page.

This banner advertisement was non-compliant:

- Pricing: No cost or frequency of billing displayed;
- No subscription reference displayed;
- No 18+ reference.

The user was directed to the Phonegenie subscription service landing page (in the background in the second browser window/tab). The landing page is non-compliant:

- Subscription reference not immediately adjacent to the call to action button;
- Pricing and billing frequency not immediately adjacent to the call to action button;
- Terms and conditions displayed at the bottom of the page (too many line spacing between call to action button and terms and conditions);
- This landing page opened in the background – tester did not click on a banner related to this service;
- If a banner directed to this service, it was an adult banner directing to a non-adult service.
-

The user clicks on the green ‘Continue’ call to action button on the service landing page. This should trigger the network hosted confirmation page where the user should be presented with the confirmation step in order to accept or reject the request to join

the Phonegenie subscription service at R5/day. The network hosted confirmation page is never displayed or visible to the user.

The user receives a Welcome Message which confirms subscription to the Phonegenie service.

WASPA CODE OF CONDUCT CLAUSES BREACHED:

4.2. Members must at all times conduct themselves in a professional manner in their dealings with the public, customers, other service providers and WASPA.

5.4. Members must have honest and fair dealings with their customers.

5.5. Members must not knowingly disseminate information that is false or deceptive, or that is likely to mislead by inaccuracy, ambiguity, exaggeration or omission.

8.2. For a subscription service, the "pricing information" consists of the word "subscription" and the cost to the customer and frequency of the billing for the service. The cost and frequency portion of the pricing information must follow the following format, with no abbreviations allowed: "RX/day", "RX/week", or "RX/month" (or RX.XX if the price includes cents). For services billed at an interval other than daily, weekly or monthly, the required format is "RX every [time period]", with no abbreviations permitted when specifying the time period. Examples of pricing information: "Subscription R5/week", "R1.50/day subscription", "RX every three days", "RX every two weeks".

8.8. Content that is promoted in advertising, must be the same content that is provided to the customer as part of the advertised service.

12.1. For any web page, pricing information does not need to be displayed for services which are free, or which are billed at standard rates. For all other services, where there is a call-to-action, pricing information must be clearly and prominently displayed immediately adjacent to the call-to-action.

12.2. There must not be any intervening text or images between the call-to-action and the pricing information. Pricing information must be legible, horizontal and presented in a way that does not require close examination. Pricing information must not be obscured by any other information. Pricing information must not be animated. It must not be a requirement that the viewer of an advert has additional software installed in order to see pricing information in the advert.

15.9. The confirmation step for any subscription service must require an explicit response from the customer of that service. The confirmation step may not be performed in an automated manner in such a way that the process is hidden from the customer.

15.10. For all subscription services initiated via a web page, there must be an additional specific confirmation step before the customer is billed. This confirmation step must be provided in one of three ways:

(i) The customer's mobile carrier may implement the confirmation step.

(ii) The member can provide the customer with a "confirmation page".

(iii) The member can send a “confirmation message” to the customer. The customer must not be charged for the confirmation message.

PACKET CAPTURE DATA:

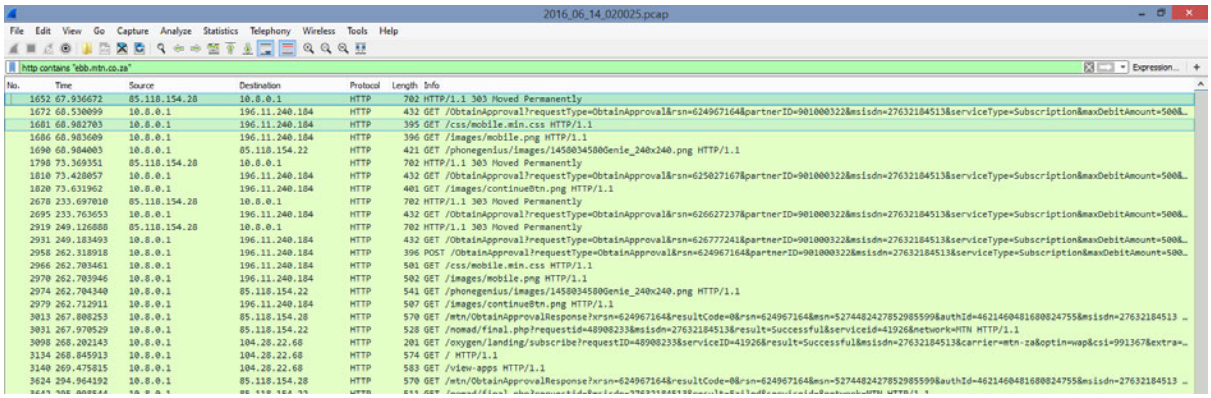
Kindly find a link to the .pcap file here: [redacted]

- This data confirms that the member’s system logged a request on the MNOs system that the MSISDN has requested to join the service.
- This should have triggered the confirmation step and the network hosted confirmation page should have been displayed (visible) to the user.
- As this page was never displayed (visible) to the user, the user could not explicitly provide consent to join the service.
- However, the data shows that there was interaction with the MNOs systems (without the user’s knowledge or consent). The network received the necessary ‘consent’ and authorised the activation of the service and provided the aggregator with permission to bill the user.
- The ‘consent’ received by the network was automated – presumably via a form of click-jacking.

How to review the logs:

- *Note: The procedure is quite technical, and if required, a technical consultant can be tasked to assist the adjudicators to interpret the logs and to decipher the content thereof.*
- Download the ‘Wireshark’ program as set out above.
- Access the .pcap file saved in the folder by following the link above.
- Once the .pcap file opens in the Wireshark program, type ‘http’ in the address bar situated at the top of the page, and then press enter.
- This will now filter the data to only display ‘http’ protocol information.
- Then type/add “contains ebb.mtn.co.za” after the ‘http’ submitted in the address bar and press enter.
- Therefore, the address bar should now read: http contains “ebb.mtn.co.za”.
- The data displayed will be the interaction with the MNO to request that a MSISDN wants to join a subscription service; the triggering and display of the network hosted confirmation page and the confirmation of acceptance of the service when the ‘Accept’ button is clicked.

This case:



- Line 3013: Request logged on the MNOs system by the member's system that the MSISDN wants to join the service. The network hosted confirmation page is triggered and 'displayed' to the user (*in casu* the user never saw this page).
- Line 3031: The acceptance of the subscription service is logged when the user 'clicked' on the 'Accept' (or similar) button (*in casu* the user never saw the network hosted confirmation page and could therefore not actively have clicked on the said button. This interaction was automated.
- Line 3098: MTN authorising the subscription service and providing the aggregator with a billing token – based on the automated acceptance of the service on the hidden network hosted confirmation page.

Subject: Non-Compliant Marketing "B1"
From: Takeo Limited [redacted]
Date: 2016-06-14 05:36 AM
To: Ziv Noy [redacted]

Hello Ziv,

We are advised of non-compliant marketing while promoting our service Phone-Genie in South Africa using explicit banners and based on the details we received we noticed that you used the attached banner on the 10th of June with the following tracking information:
- http://track.reacheffect.com/jump/?jl=2601769

We send you this request to terminate the campaign with immediate effect and to refrain from linking our servicePhone-Genie with the non-compliant marketing material with immediate effect.

We're also informing you that the payment for all the sales generated via the non-compliant marketing material will be withheld.

Best Regards,
Takeo Ltd

non-compliant-banner.png

Attachments:

non-compliant-banner.png 151 KB

TAKEO LIMITED
5 Chalfont Square, Ipswich IP4 2AJ "B2"

July 20, 2016

Dear WASPA,

In reference to the **Formal complaint notice #30975 / Takeo Limited**:

1) It is visible in the video at 1:26 that the tester clicked on the page with the continue button. The page stayed loading for over two minutes and at 3:30 it appears the tester reloaded the page. We see there another window that shows there was a previous attempt at accessing the service. Then on the third attempt the page again experienced a loading failure but this time we see a welcome message arrive. At the very end of the video we see the tester returned to the page and it was still loading. We see how the tester encountered technical failures which caused a glitch or some issues, and the tester actually was forced to input many attempts and ultimately three clicks before a successful subscription was allowed. It is these failures that had lead our affiliate to conclude that there was a glitch that caused a loop that resulted in a malfunction.

2) As mentioned above we see there is a window that was open from a previous unrecorded subscription attempt. It is impossible to see what page(s) were presented or clicked exactly because it was not recorded, and there may have been some actions that also lead to the final subscription taking place.

Because our affiliate (reacheffect) is claiming that they experienced an isolated technical failure, we present this to you now to pass their claim it was an isolated incident and that this issue had not affected multiple users.

That being said, we had already taken action to cut all ties with the affiliate. We experienced non-compliant banners from the same affiliate just the day prior to this test and as a result we terminated our relationship (see attached). The test took place at 02:00 and the affiliate traffic was stopped only a few hours later. We withheld payment and are no longer involved with them whatsoever and no longer have affiliates working on the service.

Thank you,

Takeo Limted

Dear WASPA Complaints Team,

Kindly find below the feedback to the queries raised by the Adjudicator reviewing this matter:

1. Do you attach any significance to the numerous redirects you noted at various points in the test including at time references 01:09 and 01:18?
If so, what is the significance of these redirects?

- Before any test is conducted, we clear the browsing history, cookies and cache to ensure that all previous test results are deleted in order to prevent possible cross-contamination. This ensures that the information provided is accurate and relevant to the specific service being tested.
- We used the Recordable.mobi software to capture the actual user experience.
- The video timeline was documented in writing to set out the process flow and the exact steps taken, or not taken, as the case required.
- The redirects have been captured to ensure that the member and the adjudicator can clearly see how the tester - as a representative of the end-user or consumer - moved through the process from one point to another.
- Although the consumer will very rarely pay attention to the redirects, or review the URL contained in the address bar, this information is necessary to determine what step in the process flow relates to or triggers the following step.
- Depending on the redirect details, this could provide information on, but is not limited to:
    - A consumer being directed from one part of a website to another part of the website;
    - A consumer being directed from one website to another website;
    - A consumer being directed from an advertisement to the service landing page being promoted by that advertisement;
    - A consumer clicking on a call to action button and the steps that are triggered;
    - Tracking the actions of a third party marketing suppliers (affiliate marketers) during the process;
    - Tracking when a consumer has been directed to the network hosted confirmation page, etc.;
- Very importantly, the redirect information could be used by the member to identify the third party marketing supplier that promoted the member's service in some way or form (irrespective of whether the advertising was related or unrelated, compliant or non-compliant etc.) and directed the user to the member's service landing page.
- Some of the redirects happen in less than a second – we decreased the playing speed of the video in order to capture some of the redirect details to ensure that the information provided was as accurate and detailed as possible.
- If a member makes use of third party marketing suppliers, then it is normal to see redirects from an advertisement on one site to the member's service landing page – the purpose of these affiliate marketers is to promote a service on the member's behalf in order to drive traffic to a member's offers, which the affiliate marketers are compensated for accordingly.
- Furthermore, the redirects should usually show:
    - The redirect from the service landing page to the network hosted confirmation page after the consumer clicks on the call to action button hosted on the member's service landing page;
        - As the test result clearly shows, this redirect never happened in the flow that the user experienced as set out in the video;
    - The redirect from the network hosted confirmation page after the consumer clicks on the 'Accept' or similar button on this page, controlled and managed by the network,

where the consumer confirms his or her request to join the subscription service via the second confirmation step in the Double Opt-In procedure;
    - As the user never saw the network hosted confirmation page, this redirect could not have been captured.
- 01:09 – 01:18– The tester clicked on a video on the Wetplace Website in the third browser tab/window and was redirected to a different website which opened in a fourth browser window/tab. From the information contained in the address bar it appears to be a third party marketing supplier directing the user from the banner advertisement (video) on the Wetplace Website to another destination. In this case the tester was directed to an apparent blank page (except for the almost eligible continue button) where after the process flow automatically directed the tester to the Batesk Website.

2. At various points in the video, a Phone Genie landing page loaded with a green call to action button. In order to proceed to the next stage of the process, was it necessary to tap the green button? It is unclear to me whether the video reflects this or whether it was merely sufficient to tap anywhere on the screen to trigger the next step?

- Yes, the tester has to actively click on the green call to action button in order to proceed to the next stage of the process, which should have been the display of the MTN network hosted confirmation page.
- Suggested steps to verify:
    - Open the video in the Media Player program;
    - Press the 'Play' button;
    - Right click on the video and select 'Enhancements' in the drop down menu;
    - Select 'Play speed settings' in the drop down menu;
    - Move the toggle on the spectrum to the furthest left point;
    - Use the 'forward' and 'back' buttons to navigate through the video at a slower speed;
- You will see a circle shape moving around which depicts where the tester scrolled and clicked on any buttons.
- Note: you will see that when the tester merely scrolled on the Phonegenie landing page, the non-compliant terms and conditions of the service were visible on the bottom of the screen. Once the tester actively clicks on the green call to action button, these terms and conditions disappear.

3. Takeo Limited suggested that the appropriate network hosted confirmation page may have been hidden from view by other pages which you opened during the course of the test. Is this possible?

- No, this statement is not correct or possible.
- As stated above, before any test is conducted, we clear the browsing history, cookies and cache to ensure that all previous test results are deleted in order to prevent possible cross-contamination. This ensures that the information provided is accurate and relevant to the specific service being tested.
- We used the Recordable.mobi software to capture the actual user experience.
- The video timeline was documented in writing to set out the process flow and the exact steps taken, or not taken, as the case required.
- We have in detailed steps set out what actions the tester has taken:
    - The video sets out clearly what the tester viewed and experienced. At no point during this video was any MTN network hosted confirmation page displayed to the tester, neither was it present on any of the active browser windows/tabs.
    - The steps are manually recorded in written format for ease of reference. This document sets out every step that the tester takes. Where he clicks on something,

where he closes a page, what he sees, what actions he takes, what the consequences are of each step taken etc.
    - At no point was a network hosted confirmation page visible to the tester on any of the active browser windows/tabs.
- The procedure to activate a subscription service requires certain steps – as can clearly be seen on the video and the evidence provided, all these steps were not present and therefore a legitimate subscription service could not have been activated.
- Required Procedure Flow 1: The user will browse on the internet and click on a banner advertisement promoting the subscription service. The user will be directed to the service landing page, which needs to contain certain terms and conditions. Once a user clicks on the call to action button on the service landing page, the final confirmation step is triggered and the network hosted confirmation page is displayed. Only when a user actively clicks on the 'Accept' (or similar) button on the network hosted confirmation page, will the MNO provide authorisation for the service to be activated and the aggregator will receive permission to bill the user accordingly. The user receives a welcome message to confirm that the subscription has been activated.
- The Phonegenie service landing page contains a green call to action button.
- *8.9. A "call-to-action" is any link, input box, short-code, or any other component of an advert which triggers the confirmation step for a transaction or a service.*
- Therefore, if the tester clicks on the green call to action button, this action should trigger the MTN network hosted confirmation page.
- At no point, despite the tester clicking on the green call to action button, was a MTN network hosted confirmation page displayed or visible to the user. The fact that the tester didn't see the network hosted confirmation page, means that it was impossible for the tester to complete the double opt-in procedure by clicking on the 'Accept' or similar button during the confirmation step. Therefore, no subscription service should have been activated as it is in direct contravention of Clause 15.9.
- If there was a technical failure or glitch, as alleged by the member, then the procedure should have ended with the faulty service landing page, not activated a subscription service without the required procedure being voluntarily completed by the tester.

The member stated:

- *"1) It is visible in the video at 1:26 that the tester clicked on the page with the continue button. The page stayed loading for over two minutes and at 3:30 it appears the tester reloaded the page. We see there another window that shows there was a previous attempt at accessing the service. Then on the third attempt the page again experienced a loading failure but this time we see a welcome message arrive. At the very end of the video we see the tester returned to the page and it was still loading. We see how the tester encountered technical failures which caused a glitch or some issues, and the tester actually was forced to input many attempts and ultimately three clicks before a successful subscription was allowed. It is these failures that had lead our affiliate to conclude that there was a glitch that caused a loop that resulted in a malfunction."*

- On 01:26 the tester clicks on the green call to action button – in the active second browser window/tab.
- This action should have triggered the MTN network hosted confirmation page. It did not. The page just buffered for a prolonged period.

- On 03:29 the tester clicked in the middle of the buffering page, various redirects occur and the tester is eventually redirected to another Phonegenie service landing page at approximately 03:42 – still in the active second browser window/tab. From the information in the address bar during the redirects, it appears to be a third party marketing supplier directing the tester from the buffering service landing page – which should have directed to the network hosted confirmation page – to two blank pages where after the Phonegenie service landing page is displayed again. Note: the tester did not reload the page. The tester was automatically redirected to this page again after clicking only in the middle of the buffering service landing page on 03:29.
- The member states: "*We see there another window that shows there was a previous attempt at accessing the service."* As per the video and the written record:
    - All active windows/tabs were closed when the test started;
    - The tester entered a URL in the internet application and was directed to the Wetplace Website in window 1;
    - The tester clicked on a video (banner advertisement) in active window 1 and was directed to another page of the Wetplace Website in window 2 – please note window 1 is still active in the background;
    - The tester clicked on a video (banner advertisement) in active window 2 and was directed to another page of the Wetplace Website in window 3 – please note window 1 and 2 are still active in the background;
    - The tester clicked on a video (banner advertisement) in active window 3 and was directed to another website (Batesk) in window 4 – please note window 1, window 2 and window 3 are still active in the background;
    - On 01:19 the tester closed window 4 – therefore not active anymore;
    - On 01:21 the tester closed window 3 – therefore not active anymore;
    - Only two active windows remain – window 1 and window 2;
    - The tester views the content of window 2 – the Phonegenie service landing page is displayed.
    - From 01:22 – 03:53 the tester was only operating in window 2 – window 1 was active in the background;
    - On 03:54 the tester selected the window/tab manager, two active windows (window 1 and window 2) were displayed, both relating to the Phonegenie service landing page;
    - Note: if you follow the steps back, you will see that the tester was on the Wetplace Website in window 1, clicked on a video and was redirected to window 2. When the tester clicked on a video in window 2, the tester was directed to window 3 etc. It can therefore be deduced that by clicking on the video in window 1 and later on a video in window 2 respectively, that although the tester was redirected to another window, the Phonegenie service landing page was activated and displayed on window 1 and window 2 in response to the tester clicking on the respective videos (banner advertisements).
        - Window 1 displays Wetplace Website – tester clicks on video – directed to window 2 (in background, the action of clicking on the video (banner advertisement) triggered the Phonegenie service landing page in Window 1, as displayed at 03:54);
        - Window 2 displayed the Wetplace Website – tester clicks on video – directed to window 3 (in background, the action of clicking on the video (banner

advertisement) triggered the Phonegenie service landing page in Window 2, as displayed at 03:54).

- On 03:56 the tester closed window 2 - therefore not active anymore.
- NB: only one active window remains – window 1. Any actions taken up and until this point on window 2, window 3 and window 4 are null and void. Those sessions have ended.
- On 04:06 the tester clicks on the green call to action button hosted on the Phonegenie service landing page.
- At no point is a MTN network hosted confirmation page displayed, making it impossible for the tester to voluntarily complete the double opt-in process and activate the subscription service.
- On 04:13 the tester receives a Welcome Message to confirm subscription to the Phonegenie service. The confirmation step (the MTN network confirmation page that requires a voluntary and explicit confirmation to join the service) was never displayed to, or concluded by the tester.
- From 04:07 until the buffering Phonegenie service landing page is closed at 05:02, no network hosted confirmation is displayed. This window is the ONLY active window. There are no other windows/tabs in the background.

- The member states: "*We see how the tester encountered technical failures which caused a glitch or some issues, and the tester actually was forced to input many attempts and ultimately three clicks before a successful subscription was allowed."*
  - Not one of the testers actions to click on the green call to action button triggered the MTN network hosted confirmation page to display, which would have presented the tester with the opportunity to accept or reject the request to join the Phonegenie subscription service, as is required by the WASPA Code of Conduct;
  - This confirmation step was automated in a manner that was not known, or visible, to the tester;
  - Three clicks of the green call to action button on the Phonegenie service landing page should not activate a subscription – the procedure should end there if there is a technical issue and not automatically activate a subscription service or bypass the required steps and procedures.
- The procedure is simple for flow 1: the tester should on two respective occasions be made aware of the billing information and actively and voluntarily confirm their request to join the service at each step of the double opt-in process – one step being the landing page and the second the network hosted confirmation page. The second step was not displayed or visible to the user and therefore a legitimate subscription could not have been activated.

The member stated:

- "2. *As mentioned above we see there is a window that was open from a previous unrecorded subscription attempt. It is impossible to see what page(s) were presented or clicked exactly because it was not recorded, and there may have been some actions that also lead to the final subscription taking place."*
- This is factually incorrect.
- After the tester closed window 3 and window 4, two windows remained active. When the tester used the window/tab manager to review the two active windows, both had content on it relating to the Phonegenie subscription service. As stated above, these pages were activated when the testers clicked on videos (banner advertisements) contained on the Wetplace Website which triggered these pages on window 1 and window 2 respectively.

- Therefore, the content on window 1 and window 2 was not from a 'previous unrecorded subscription attempt…', but was in fact part of the test that forms the basis of this complaint. All the evidence is clearly recorded, and both the video and written record sets out the actions taken.
- The allegation that previous tests information (previous unrecorded subscription attempts) was mixed with the results of the current test under review, is factually incorrect and we specifically deny it.
- In conclusion:
    - At the end of the test when the Welcome Message is received, only one window was active.
    - This window contained the buffering Phonegenie service landing page.
    - There is no other window that could have hosted/displayed/contained the MTN network hosted confirmation page. For clarity, there is no window visible to the tester – if such a window was to be found anywhere, it was masked/disguised/hidden to not be seen by the tester.
    - The questions: ***Takeo Limited suggested that the appropriate network hosted confirmation page may have been hidden from view by other pages which you opened during the course of the test. Is this possible?***
    - Even if, which we specifically deny was the case, the network hosted confirmation page was hidden from view by other pages opened during the course of the test (note: only one window active when the subscription service was activated and the Welcome Message received), the tester needed to actively and voluntarily confirm the subscription on this page. If it was 'hidden', then this step was impossible to complete and no subscription should have been activated. Either way, this step was automated without the tester's knowledge or explicit consent.

We trust that the above information clarifies the queries raised by the Adjudicator.

If there are any further or related questions, we will attend to them accordingly.

Kind Regards,
WASPA Media Monitoring Team