Wireless Application Service Providers' Association

Report of the Adjudicator

Complaint number	**#33582**
Cited WASPA members	**Freenet digital Gmbh (1515)**
Notifiable WASPA members	All
Source of the complaint	WASPA Media Monitor
Complaint short description	Failure to ensure adequate pricing of Subscription Service and confirmation steps and pages inaccurate.
Date complaint lodged	24 April 2017
Date of alleged breach	21 April 2017
Applicable version of the Code	14.7
Clauses of the Code cited	*4*.2., 5.4., 5.5., 8.2., 15.9., 15.10.(i,ii,iii), 15.11.(ae)
Related complaints considered	**31002** **30975**
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, 8.2, 15.9, 15.10 and 15.11 of the Code.
Other sanctions	Full Refund to all affected subscribers/ customers;
Is this report notable?	Not Notable
Summary of notability	N/A

Initial complaint

The complaint was lodged with WASPA via the WASPA website and the below complaint was sent to respondent and aggregators on 24 April 2017.

The MM team received a video capture file, from our supplier MCP. The video file displays a click jacking scenario.

The test was performed on: MSISDN 27872405426, GMT 12:26, 21st April 2017.This complaint is of a very serious nature and utmost priority is required from Freenet Digital (Information Provider) and Oxygen 8 (Aggregator).

User journey recorded as follows:

MCP browsed the xxx website known as eroXIA.com, which displayed a floating banner on the bottom of the web page. They clicked on the banner.

They opened the floating banner in a new window which directed them to a solid white page, which had a black box. It looked like a "video loading" window, which seemed to be buffering/loading a video. No video however loaded.

They then received a Welcome SMS for the service Bitbop (Freenet Digital). They were able to visit the service homepage, by clicking on the URL provided in the Welcome SMS.

At no instance was a Landing page or a Network hosted Confirmation page presented to the user. A user viewing the different categories of the Subscription Service, MCP then cancelled the Service within the service homepage.

The unsub was confirmed.

Member's response

The respondent provided a response to the complaint on 24 April 2017 (due to initial emergency panel hearing):*

Confirmation of receipt of email regarding complaint, complaint taken very seriously and we are committed to respond to the complaint as well as ensure high level of transparency and cooperativeness.

In mitigation, the incident was discovered due to internal auditing on 20th April and resolved as the investigation indicated that the same ad partner was linked to the orders. [Attached Appendix A].The sales team therefore immediately informed the network to stop the campaign immediately

and such was confirmed, there are no such campaigns which are live. Fraudulent campaigns have never been mandated by our company and our contracts with partner networks contain compliance requirements which may authorise the sanctioning of such behaviour. The partner network was sent an official warning letter reminding them of the contractual obligations and the legal situation. We distribute regularly our partner newsletter that further covers all aspects of regulation in the market. Partner networks are diligently selected and instructed on legal requirements and sanctions as well as we have an active fraud prevention programme and are on constant exchange with tech experts. We have an open dialogue with the anti- fraud department of the British Regulator PSA, and the German Auditor MDK GmbH., constantly adjust safety precautions as well as keep them up to date.

We have already de registered all affected customers and will do a full refund to any of them.

(*please note that the above is a summarised version of response)

Complainant's response

The Respondents submissions were sent to complainant for a response on 24 April 2017 as well as on the 05 May 2017.

The complainant failed and / or neglected to respond to the Respondents submissions provided, presumably due to the initial emergency panel set up / situation.

Member's further response

The respondent then made a further response on the 05 May 2017, as advised below:*

We accept the downgrade of the complaint, as well as submit the same information as provided on the 24 April 2017, along with various further submissions. The video sent as an attachment which indicated an incompliant orderflow, and the telephone number shown evidently didn't sign up with our service. This was not registered through our service provider nor aggregator and is therefore not a customer. We wonder if this audit was mistaken by MCP or if any other technical or fraudulent provider was linked to this flow which made us appear on the screen alternatively another provider is profiting to our disadvantage from the sale. Kindly verify this. The alternate number provided we note in our logs on our customer database, however no evidence of such fraud. Our audit was what allowed us to immediately react prior to the involvement of MCP or WASPA and we highly appreciate if the independent adjudicator would take this proactive action into consideration.

(*please note that the above is a summarised version of response)

Sections of the Code considered

The following sections of the WASPA Code of Conduct, version 14.7, were considered:

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 abbreviation 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 [_me period]”, with no abbreviations premised when specifying the _me period. Examples of pricing information: “Subscription R5/week”, “R1.50/day subscription”, “RX every three days”, “RX every two weeks”.

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.

15.11. A confirmation page must contain the following information:

(a) the name of the service,

(b) the pricing information,

(c) a customer support number,

(d) Instructions for confirming the initiation of the subscription service, and

(e) a link to any applicable terms and conditions.

Additional information about the service may also be included, provided it follows the above information.

Decision

My submission is the following:

The Complaint is upheld due to various reasons which I shall not hesitate to outline, I am reminded of the introduction to the Code of Conduct, *"WASPA aims to ensure that consumers receive world-class services and that members operate according to ethical and reasonable business practices"* as well as the following , "*The primary objective of the WASPA Code of Conduct is to ensure that members of the public can use mobile services with confidence, assured that they will be provided with accurate information about all services and the pricing associated with those services*".

The primary objective of WASPA may be to ensure that members of the public are confident in their use of an accurate service as well as pricing which is accurate, but this is a self-regulatory body wherein members must ensure that they operate reasonable business practice, now those of you who have studied law will understand and explain that the "*reasonable test*" is one which is ever evolving and never certain, it is a test which sees one "thing" measured against the next, but such thing must most comparatively exercise average care, skill, and judgment in conduct.

The Respondent has made available a newsletter sent to all partners and one portion of such is an update of national / international regulations as well as an entire paragraph that states,

> **AUDITS**
>
> Mobile Carriers, regulators and we ourselves as a content provider are consequently monitoring the mobile ad market through various auditing companies worldwide. In order to make sure that the rules are followed and in order to prevent consumer harm, Carriers and regulators have implemented a strict sanctioning scheme for any wrongdoing they discover. Detected rule infringements are reported nearly in real time and may lead into suspensions and fines depending from the severeness of the offence. We as the content provider expect ad partner´s full cooperation in case anything gets reported.

This is acceptable and a business practice which denotes a focus on keeping the end user in mind, however their systems failed in the current situation and as such the result must be a sanction. While the Respondents auditors had already discovered that the order was without any human interface and had made the Network partner aware of this on the 20th April 2017 through their own internal audit mechanisms and advised the said partner to cease such campaigns, they went a step further and out of their own, penalized that partner for what they feared could possibly jeopardize the entire business and retained any CPA that was generated by that company hence the sanction is one that is acceptable to what must already have been generated.

I will not reiterate the outcome and submissions made by the Adjudicators under complaint #31002 and #30975 but I have largely based my decision/ outcome on the two and as such the

submissions made are relevant in that, in #30975, the service was called Phonegenie and involved offers of adult content which was triggered by clicking on a banner ad. The end result of a somewhat convoluted process was that the consumer was subscribed to the service and received a subscription confirmation message, one must note further that, in #31002 the Adjudicator indicated the following "*Whether the subscription was facilitated by clickjacking or a Javascript Same Origin Bypass is unclear and largely irrelevant to the outcome. The simple fact is that the Monitor's phone was subscribed to the service without authorising the subscription on a network-hosted subscription confirmation page, at the very least. In fact, there didn't appear to be even an initial subscription opt-in call to action that the Monitor activated, either. The effect of this is that simply clicking to view content activated what should have been a double opt-in subscription mechanism"*

I need to state that the situation placed before me (*while already remedied by the Respondent prior to our intervention*) is appalling, *"Clickjacking—the practice of deceptively directing a website visitor's clicks to an undesired element of another site—is surprisingly effective. It's been often used to propagate links to malicious websites on Facebook. More recently, similar techniques have been shown effective in de-anonymizing website visitors and even tricking them into granting attackers access to OAuth-secured data."* The assessment of this situation is that it further is an exploit in which malicious coding is hidden beneath apparently legitimate buttons or other clickable content on a website.

My submission is that there has been a breach of all the clauses listed in the initial complaint, while we do consider the Respondents factors and/ or evidence in mitigation, we advise and remind the Respondent that members must always have honest and fair dealings with their customers. Evidence was placed before me by the Respondent that the MSISDN used is unknown, there is no actual proof and as such the video orderflow remains the reasoning behind the imposition of the sanction.

In final submission the time frames are primarily the reasoning behind the awarding of the sanction, the Respondent advised that he became aware on the 20th April 2017 and paused the campaign, the test conducted for the MM was done on the 21st April 2017 indicative that the "pause" was ineffective (*even though the evidence was that no such campaigns were live*) and as such the service still manged to breach the code clauses applicable in its entirety.

Sanctions

A fine in the amount of R100 000 in respect of the member's breaches of sections 4.2, 5.4, 5.5, 8.2, 15.9, 15.10 and 15.11 of the Code.

The amount of R 100 000, 00 is payable by the Respondent within 7 (seven) days of receipt of this Adjudication.

Other Sanctions:

1. Full Refund to all affected subscribers/ customers within 24 hours of receipt of this adjudication report.

Matters referred back to WASPA

"We wonder if this audit was mistaken by MCP or if any other technical or fraudulent provider was linked to this flow which made us appear on the screen alternatively another provider is profiting to our disadvantage from the sale. Kindly verify this" – this was placed as evidence before me by the Respondent, which cannot be ignored and I therefore direct that the MM conduct further detailed and technical tests.
