W A S P A

Wireless Application Service Providers' Association

Report of the Adjudicator

Complaint number	#39143
Cited WASPA members	Worldplay (0015)
Notifiable WASPA members	none
Source of the complaint	WASPA Compliance Department.
Complaint short description	Non Implementation of fraud prevention measures
Date complaint lodged	18 May 2018
Date of alleged breach	Unknown

Applicable version of the Code	15. 5
Clauses of the Code cited	4.11 (a)
Related complaints considered	None.
Fines imposed	R 100 000,00 (One hundred thousand rand) payable and R 50 000,00 (Fifty thousand rand) Suspended for six months from date of publication of adjudication: R 150 000,00 for breach of clause 4.11 (a)
Other sanctions	None.
Is this report notable?	Notable
Summary of notability	*Compliance with the Fraud detection and mitigation document in accordance with WASPA code of good practice should be pivotal to all in the industry as non-compliance would mean detrimental consequence to all. Regular fraud parameters must be set up and tested by WASPs.*

Initial complaint

WASPA conducted a test on Worldplay – Cellon and identified that you have failed/omitted to implement the requirements as set out in Section 2.3 of the Fraud Detection and Mitigation Best Practice Guidelines.

Your systems are therefore vulnerable and have not been sufficiently secured to prevent potential fraudulent attacks or activity.

- Content Security Policy Directive

- X-Frame Options Response Headers

- 302 Redirect

As such, you are potentially in breach of Clause 4.11(a) of the WASPA Code of Conduct.

We request you to take immediate action to rectify this breach and to align your systems with the procedures as set out in the Fraud Detection and Mitigation Best Practice Guidelines.

Please provide proof of the actions taken in order to comply with the requirements to secure your systems.

Note: **URGENT ATTENTION** is required. Any delay in implementing the required practices may be considered as an aggravating factor for this specific potential breach.

Member’s response

The respondent failed to respond to the formal complaint and requested the complaints team recant the formal complaint based on screen shots of the header received marked 18. Further the respondent indicated that she is unsure as to where the confusion is coming from.

Complainant’s response

NONE.

Member’s further response

Respondent provided no response, however requested a recant of the complaint.

On the 02 July 2018, the Respondent provided a response noting that this is in fact a formal complaint that is at the liberty of an independent adjudicator and provided a response when promoted by the secretariat.

See attached, Respondent Response marked **Annexure A**.

Sections of the Code considered

The following sections of the WASPA Code of Conduct, version 15.5, were considered:

4.11. Members must take reasonable steps to prevent their networks and systems from being used in a fraudulent manner, including:

(a) complying with WASPA's published best practices for fraud prevention

---

Decision

I note a failure on the part of the Respondent to adhere to a request provided by the Compliance Department, which reads as follows;

Please provide proof of the actions taken in order to comply with the requirements to secure your systems.

Note: URGENT ATTENTION is required. Any delay in implementing the required practices may be considered as an aggravating factor for this specific potential breach

The reasoning behind the bold, italicized and highlighted portion is to indicate to the Respondent (*and all respondents*) that it is imperative to read the entire complaint and to, at the very least be less derisive with their response.

The complainant has placed on record that:

WASPA conducted a test on Worldplay – Cellon and identified that you have failed/omitted to implement the requirements as set out in Section 2.3 of the Fraud Detection and Mitigation Best Practice Guidelines.

Your systems are therefore vulnerable and have not been sufficiently secured to prevent potential fraudulent attacks or activity.

And the response from the Respondent was:

Please recant - the screen shots you provided clearly show that we are compliant so I am not sure where the confusion is coming from? (Red below)

I must highlight that, I am unable to consider any related published complaints as there are none, therefore this concept of fraud via click jacking and / or malware (harmful applications) may just be on the rise as a new phenomenon and the industry as a whole is in danger.

My submissions and findings are based on both the Fraud Detection and Mitigation Policy Document (that *all WASPs were advised of from April 2017 and which has already seen over 13 versions come into existence, with version 2.1 being the latest*) and the WASPA Code of Conduct *"Code"*.

Clickjacking works by iframing or otherwise dynamically embedding a page into another page, overlaying it with different content and passing clicks down to the iframed target. That allows attackers to trick users to click on buttons without seeing pricing or generally being aware they are following a purchase flow. We are all well aware that the use of technology in our daily lives has been growing rapidly, more so with persons making use of the web and applications to assist in most tasks.

I do concede and concur with the respondent that, they have, in good faith ensured that there is the correct fraud implementation and functionality within their system and it is for that reason that I find that there is no actual fraud that occurred while their headers were incorrectly set.

The respondent, states in the response that there was in fact compliance (*The WASPA anti-fraud rules are asking for these headers to be set to "NONE" and "DENY" respectively, which will lead to pages being framed to not display upon rendering*) and we concur but not entirely in that on the 01 May 2018 (shortened log attached, highlighted and marked **Annexure B**) , there is a 302 Error code , incorrectly as this 302 HTTP status code indicates redirection instead of being code 200 which would indicate page rendering.

Clause 2.3 of the Fraud detection and mitigation practice best practice document, specifically states the following:

" to be clear and to ensure easy enforceability, a page on the domain used immediately before the Network Hosted Confirmation Page should:

- ***include all the relevant HTTP headers as discussed in section 2.3***
- ***incude the javascript as discussed in section 2.3***
- ***be served with an HTTP 200 …"***

it must be highlighted to the Respondent, that the Network Confirmation page was not secured under **Annexure B**.

While it is taken in good faith that fraud measures are implemented in accordance with clause 4.11(a) read with sub clause 2.3 of version 2.1 of the Fraud detection and mitigation practice best practice document, by the Respondent. This exercise must be a careful and continuous one as there may be a possibility that they could not prevent clickjacking. In other words, all doors must be secured. I pause to note that should there have been actual fraud, a higher sanction would have been imposed.

Sanctions

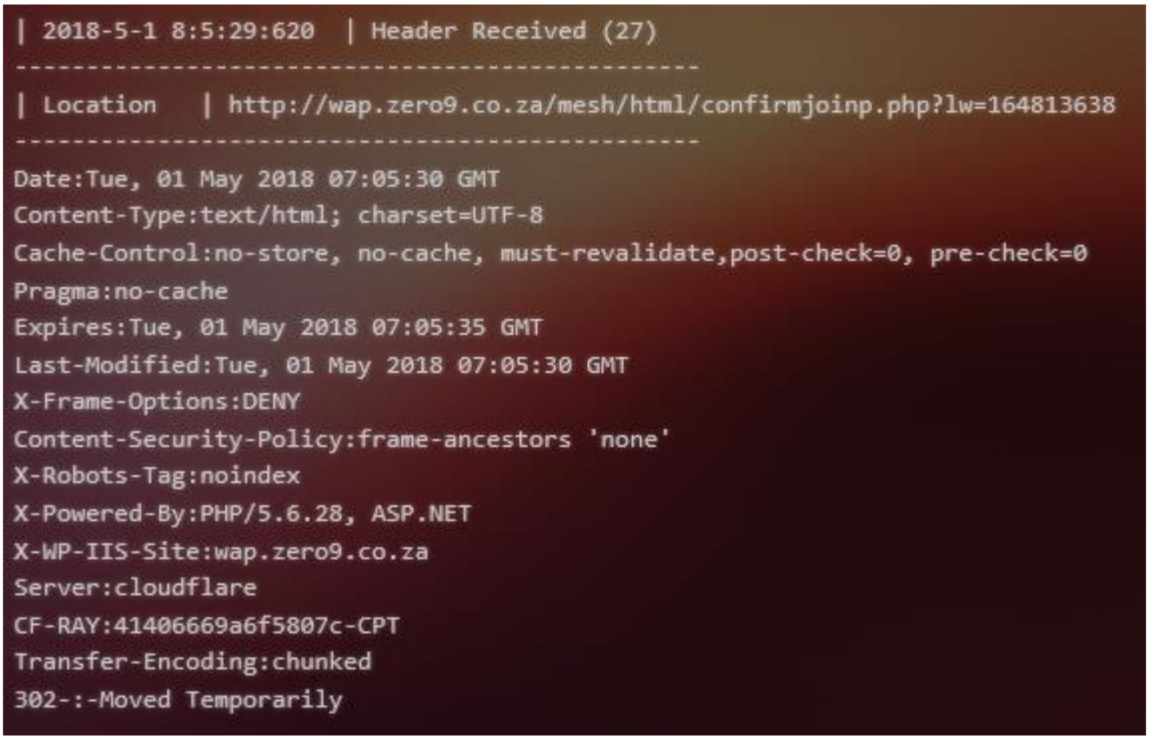
I therefore determine that there was in fact a breach of the code, therefore the cited clause contravention is upheld and I call for the following fine to be imposed on the Respondent, such fine is therefore payable within 7(seven) days of receipt of the adjudication report, and the suspended portion is so suspended for a period of 6 (six) months from date of publication of the report. Should the Respondent breach the cited clause within the six month period, the amount so suspended shall be immediately due and payable.

All fines are directly imposed on Worldplay (0015).

R 150 000, 00 for breach of clause 4.11(a), R 50 000, 00 of which is to be suspended for a period of six months.

Matters referred back to WASPA

NONE.



```
| 2018-5-1 8:5:29:620  | Header Received (27)
------------------------------------------------
| Location   | http://wap.zero9.co.za/mesh/html/confirmjoinp.php?lw=164813638
------------------------------------------------
Date:Tue, 01 May 2018 07:05:30 GMT
Content-Type:text/html; charset=UTF-8
Cache-Control:no-store, no-cache, must-revalidate,post-check=0, pre-check=0
Pragma:no-cache
Expires:Tue, 01 May 2018 07:05:35 GMT
Last-Modified:Tue, 01 May 2018 07:05:30 GMT
X-Frame-Options:DENY
Content-Security-Policy:frame-ancestors 'none'
X-Robots-Tag:noindex
X-Powered-By:PHP/5.6.28, ASP.NET
X-WP-IIS-Site:wap.zero9.co.za
Server:cloudflare
CF-RAY:41406669a6f5807c-CPT
Transfer-Encoding:chunked
302-:-Moved Temporarily
```

adjudication without a further submission from the complainant
From: [redacted]
Date: 2018-07-02 05:17 PM
To: "<complaints@waspa.org.za>" <complaints@waspa.org.za>
CC: [redacted]@waspa.org.za>, archive@waspa.org.za

Good day WASPA

I trust this finds you well.

Given that no clarity was given by WASPA as requested by myself given my confusion as to why we received this complaint questioning our compliancy to section 2.3 when if fact compliancy is proved in the screen shots shared by you, my question/concerns raised and not answered did not constitute an official response from myself - I therefore would like to provide the following in response to your original complaint, given that this has moved forward to an adjudication much to my surprise. Here we go once again;

Complaint;

> *[...] you have failed/omitted to implement the requirements as set out in Section 2.3 [...]*
> *• Content Security Policy Directive*
> *• X-Frame Options Response Headers*
> *• 302 Redirect*

Yet it is clear from the information you provided that the pages we serve do include both the Content-Security-Policy and the X-Frame-Options response headers.

Open any one of the *-screenshot-* PDFs and they all clearly show this.
Here is 1-May-2018-Screenshot.pdf for example: