Wireless Application Service Providers' Association

Report of the Adjudicator

Complaint number	#39142
Cited WASPA members	Hammer Mobile Limited (1485)
Notifiable WASPA members	Basebone Pty Ltd (1344)
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	15. 5

the Code	
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 HAMMER MOBILE – DOWNLOUZ 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

Dear WASPA Secretariat,

Ref.: Formal Complaint #39142 Hammer Mobile Ltd.

WHEREAS, we have become aware that several WASPs have had cases lodged based on the exact same arguments (#39136 Hulkmobile Ltd and #39135 Westbound Direct Ltd);

WHEREAS, based on the technical details provided by the WASPA Monitoring Team, we have instructed our technical department to analyze the issue at hand and provide proper explanation in order to clarify the reason why our Anti-fraud solution was not fully compliant with the relevant WASPA "Fraud Detection and Mitigation" requirements;

NOW THEREFORE, we herewith reply to our Formal Complaint #39142 referenced above, providing all the information we consider relevant to the case.

By analyzing the WASPA technical report, what our Tech Team has observed is that, in our Fraud Detection solution, the headers "Content-Security-Policy" and "X-Frame-Options" were set respectively to Frame-ancestors "self'" and "SAMEORIGIN".

The purpose of the headers "Content-Security-Policy" and "X-Frame-Options" are to deny third parties to iframe Landing and Confirmation pages and consequently overlay those pages (in modern browsers).

We have immediately crosschecked the above-mentioned setting options with the actual requirements of the WASPA “Fraud Detection and Mitigation” document and unfortunately our Anti-Fraud Tool was not complying with the due settings, being that 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. Moreover, the HTTP status code was “302”, indicating redirection instead of being code “200” indicating page rendering.

Unfortunately, we have to admit that this has been a technical implementation error on our end. In facts the two HTTP headers only take effect with page rendering. Since no page was displayed, they were not able to prevent clickjacking.

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 would like nevertheless to underline that we were not aware of this condition on our AntiFraud Tool and that upon receipt of WASPA Monitoring Team heads up, we have immediately proceeded ensuring pages display in all cases in order to block any attempt of fraudulent interaction.

Moreover, we have adjusted the clickjacking headers to “NONE” and “DENY”, respectively, in order to fully comply with the WASPA “Fraud Detection and Mitigation” specifications.

Concluding on this matter, this was clearly a technical implementation error on our side and we assume the liability of the same. Nevertheless, we would like to clarify that we were operating in bona fide and that as soon as we have been informed by WASPA about this issue we have immediately reacted and taken the relevant due actions.

We therefore ask the Adjudicator to consider the following mitigating factors:

- Our behavior on this matter has been fully collaborative since the very beginning;

- The shortcoming was actually due to a human error in the implementation of a fairly complicated technical measure;

- We have acknowledged our error and worked on the same in order to prevent any further issue in the future;

- The due technical actions have been taken immediately as per WASPA Monitoring Team request.

We trust you find the above in order.

Complainant’s response

NONE.

Member’s further response

Dear WASPA

We are pleased to submit our response to the complaint in subject.

Regards

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 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”*.

While other WASPs fail at basic responses and provision of palatable information, I commend this WASP for ensuring that they adequately respond to the secretariat and ensure that they are in fact adhering to what is required as per the response by the secretariat.

I concur with the Respondent that, *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.

The complainant has placed on record that:

"…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 detailed and well thought of, however the Respondent has made concessions that cannot be ignored;

"….we have instructed our technical department to analyze the issue at hand and provide proper explanation in order to clarify the reason why our Anti-fraud solution was not fully compliant with the relevant WASPA "Fraud Detection and Mitigation" requirements…"

"….our Tech Team has observed is that, in our Fraud Detection solution, the headers "Content-Security-Policy" and "X-Frame-Options" were set respectively to Frame-ancestors "self'" and "SAMEORIGIN"…."

"…unfortunately our Anti-Fraud Tool was not complying with the due settings, being that 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. Moreover, the HTTP status code was "302", indicating redirection instead of being code "200" indicating page rendering…"

"…Unfortunately, we have to admit that this has been a technical implementation error on our end…"

However, I do concede and concur with the respondent that, they have, in good faith attended to this issue and 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.

It must be submitted that more responsibility must be taken as to ensure 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 continuously and that the two HTTP headers only take effect with page rendering and since no page was displayed at the time when the testing took pace they were not able to prevent clickjacking.   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 Hammer Mobile Limited (1485).

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.
